(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－285623
（P2001－285623A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
H04N	1/387		H04N	1/387	5B057
G06T	1/00	500	G06T	1/00	500B 5C063
G10L	11/00		G10L	9/00	E 5C076
H04N	7/08		H04N	7/08	Z
	7/081				

審査請求　未請求　請求項の数31　ＯＬ　（全 34 頁）

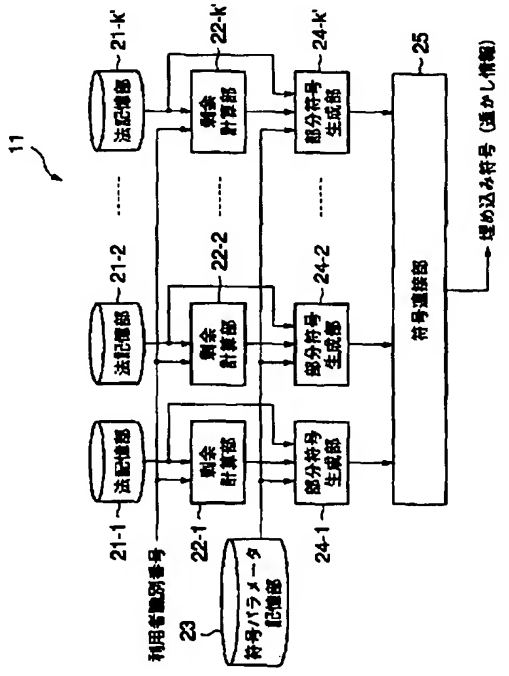
(21)出願番号　特願2000－263872(P2000－263872)
(22)出願日　平成12年８月31日(2000.8.31)
(31)優先権主張番号　特願平11－280652
(32)優先日　平成11年９月30日(1999.9.30)
(33)優先権主張国　日本（ＪＰ）
(31)優先権主張番号　特願2000－16285(P2000－16285)
(32)優先日　平成12年１月25日(2000.1.25)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000003078
株式会社東芝
東京都港区芝浦一丁目１番１号
(72)発明者　村谷　博文
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　埋め込み符号生成方法及び装置、埋め込み符号検出方法及び装置並びに電子透かし埋め込み装置及び電子透かし検出装置

(57)【要約】
【課題】結託攻撃への耐性を持ち、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えた透かし情報として埋め込まれる埋め込み符号生成装置を提供する。
【解決手段】剰余計算部２２－１，２２－２，…，２２－ｋ′により利用者ＩＤに対して法記憶部２１－１，２１－２，…，２１－ｋ′に記憶された互いに素の関係にある複数の整数を法とする剰余をそれぞれ求め、これらの剰余及び符号化パラメータ記憶部２３に記憶されたパラメータに基づいて、成分符号生成部２４－１，２４－２，…，２４－ｋ′により所定のビット数を一単位とする連続した１の列及び０の列で構成される成分符号をそれぞれ生成し、これらの各成分符号を連接部２５で連接して、透かし情報を構成する埋め込み符号を生成する。



1

【特許請求の範囲】

【請求項１】所定のコンテンツに埋め込まれるべき埋め込み符号を生成する埋め込み符号生成方法において、

前記コンテンツを利用する利用者の利用者識別番号に対して、互いに素の関係にある複数の整数を法とする複数の剰余を計算する剰余計算ステップと、

前記剰余計算手段により求められた各剰余を表す複数の成分符号を生成する成分符号生成ステップと、

前記成分符号生成手段により生成された各成分符号を連接して前記埋め込み符号を生成する連接ステップとを具備する埋め込み符号生成方法。

【請求項２】所定のコンテンツに埋め込まれるべき埋め込み符号を生成する埋め込み符号生成装置において、

前記コンテンツを利用する利用者の利用者識別番号に対して、互いに素の関係にある複数の整数を法とする複数の剰余を計算する剰余計算手段と、

前記剰余計算手段により求められた各剰余を表す複数の成分符号を生成する成分符号生成手段と、

前記成分符号生成手段により生成された各成分符号を連接して前記埋め込み符号を生成する連接手段とを具備する埋め込み符号生成装置。

【請求項３】前記成分符号生成手段は、前記複数の成分符号として所定のビット数を一単位とする連続した１の列及び０の列で構成される符号を生成する請求項２記載の埋め込み符号生成装置。

【請求項４】所定のコンテンツに埋め込まれた、複数の成分符号を連接した埋め込み符号を検出する埋め込み符号検出方法において、

前記埋め込み符号を前記複数の成分符号に分割する符号分割ステップと、

分割された各成分符号をそれぞれ復号して予め定められた互いに素の関係にある複数の整数を法とする２つの剰余からなる複数の剰余対を得る成分符号復号ステップと、

前記複数の剰余対から前記コンテンツに対して結託攻撃を行った結託者の利用者識別番号を計算する結託者番号計算ステップとを具備する埋め込み符号検出方法。

【請求項５】所定のコンテンツに埋め込まれた複数の成分符号を連接した埋め込み符号を検出する埋め込み符号検出装置において、

前記埋め込み符号を前記複数の成分符号に分割する符号分割手段と、

分割された各成分符号をそれぞれ復号して予め定められた互いに素の関係にある複数の整数を法とする２つの剰余からなる複数の剰余対を得る成分符号復号手段と、

前記複数の剰余対から前記コンテンツに対して結託攻撃を行った結託者の利用者識別番号を計算する結託者番号計算手段とを具備する埋め込み符号検出装置。

【請求項６】前記複数の成分符号は、所定のビット数を一単位とする連続した１の列及び０の列で構成される請

2

求項５記載の埋め込み符号検出装置。

【請求項７】前記複数の剰余対から結託の有無を判定する結託判定手段をさらに有し、前記結託者番号計算手段は該結託判定手段により結託があると判定されたとき前記結託者の利用者識別番号を計算する請求項５記載の埋め込み符号検出装置。

【請求項８】前記結託者番号計算手段は、入力されたｋ′個の剰余対の各々から一方の剰余を選択してｋ′個の剰余の組（Ｒ１，Ｒ２，…，Ｒｋ′）を生成する剰余選択部と、

前記剰余選択部により生成されたｋ′個の剰余の組から選択された相異なるｋ個の剰余（Ｓ１，Ｓ２，…，Ｓｋ）から中国剰余定理に従って結託者の利用者識別番号ｕの候補を計算する中国剰余定理部と、

前記剰余選択部により生成されたｋ′個の剰余の組から前記ｋ個の剰余を選択して前記中国剰余定理部に渡し、前記中国剰余定理部により計算された結託者の利用者識別番号候補ｕの候補から該結託者の利用者識別番号を特定して出力する一貫性検査部とを含み、

前記一貫性検査部は、前記剰余選択部により生成されたｋ′個の剰余の組から前記ｋ個の剰余を選択する選択処理と、前記中国剰余定理部により計算された結託者の利用者識別番号ｕの候補と残りの（ｋ′－ｋ）個の剰余のうちの所定個数（ｙ）の剰余との間に$Ri = u \bmod p_i$（$i = i_1, i_2, \cdots, i_z$）の関係が成立するか否かを判定する判定処理と、該判定処理により前記関係が成立する場合に結託者の利用者識別番号として出力する出力処理とを有し、

前記関係が成立しない場合には前記剰余選択部により生成されたｋ′個の剰余の組から前記選択処理により新たな組み合わせのｋ個の剰余（Ｓ１，Ｓ２，…，Ｓｋ）を選択して前記判定処理を行い、全ての組み合わせのｋ個の剰余（Ｓ１，Ｓ２，…，Ｓｋ）に対して前記関係が成立しない場合には前記剰余選択部に対して新たなｋ′個の剰余の組を要求して、前記関係が成立するまで前記選択処理及び判定処理を繰り返す請求項５記載の埋め込み符号検出装置。

【請求項９】入力された利用者識別番号に対応して複数の整数要素の組を計算する計算手段と、

所定個数の利用者識別番号に対して前記計算手段により計算される全ての整数要素の組を表現可能なｋ′個の成分符号のうちのｋ個の組み合わせが前記利用者識別番号を一意に表現できる成分符号を前記各整数要素に対応してそれぞれ生成する成分符号生成手段と、

前記成分符号生成手段により生成された各成分符号を連接して埋め込み符号を生成する連接手段とを具備し、

前記ｋ′は、３以上の正整数をｃ、１以上の正整数をｚ、前記埋め込み符号の検出時に前記各成分符号から検出できる前記整数要素の個数をｑとして、ｃ（ｋ＋ｚ）／ｑ以上となるように決定されている埋込み符号生成装

3

置。

【請求項１０】前記所定個数の利用者識別番号に対して前記計算手段により計算される各整数要素のとりうる値の個数をp_i（ｉ＝１，２，…，ｋ′）とし、前記埋め込＊

$$\left[1-\prod_{i=1}^{z}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{c(k+z)/2^{Ci+zX2^{k+z}}} \geq 1-\frac{\varepsilon}{2} \qquad (1)$$

の条件を満たすように設定されている請求項９記載の埋め込み符号生成装置。

【請求項１１】前記計算手段は、前記入力された利用者識別番号に対応して互いに素の関係にある複数の整数を法とする剰余の組を前記整数要素の組として計算する請求項９記載の埋め込み符号生成装置。

【請求項１２】前記計算手段は、前記入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算※

$$k' = \frac{c}{2}(k+z) \leq \frac{p^k - 1}{p-1} \qquad (2)$$

の条件をさらに満たす請求項９記載の埋め込み符号生成装置。

【請求項１４】所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能なｋ′個の成分符号のうちのｋ個の組み合わせが利用者識別番号を一意に表現できる成分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、

抽出された各成分符号に分割する符号分割手段と、

分割された各成分符号をそれぞれ復号する成分符号復号手段と、★

$$\left[1-\prod_{i=1}^{z}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{c(k+z)/2^{Ci+zX2^{k+z}}} \geq 1-\frac{\varepsilon}{2} \qquad (1)$$

の条件を満たすように設定されている請求項１４記載の埋め込み符号検出装置。

【請求項１６】前記整数要素の組は、前記利用者識別番号に対応して計算された互いに素の関係にある複数の整数を法とする剰余の組である請求項１４記載の埋め込み符号検出装置。

【請求項１７】前記整数要素の組は、前記利用者識別番号に対応して計算された平行移動によって定義される同☆

$$k' = \frac{c}{2}(k+z) \leq \frac{p^k - 1}{p-1} \qquad (2)$$

の条件をさらに満たす請求項１４記載の埋め込み符号検出装置。

4

＊み符号の検出時に想定される検出誤り率をεとしたとき、前記ｋ′は、

【数１】

【数２】

【数３】

【数４】

※する請求項９記載の埋め込み符号生成装置。

【請求項１３】前記計算手段は、前記入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算するものであり、

前記p_i（ｉ＝１，２，…，ｋ′）を同一の正整数ｐとして、

★各成分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、

前記ｋ′は、３以上の正整数をｃ、１以上の正整数をｚ、前記埋め込み符号の検出時に前記各成分符号から検出できる前記整数要素の個数をｑとして、ｃ（ｋ＋ｚ）／ｑ以上となるように決定されている埋込み符号検出装置。

【請求項１５】前記所定個数の利用者識別番号に対して計算される各整数要素のとりうる値をp_i（ｉ＝１，２，…，ｋ′）とし、前記埋め込み符号の検出時に想定される検出誤り率をεとしたとき、前記ｋ′は、

☆値類に属する要素の番号の組である請求項１４記載の埋め込み符号検出装置。

【請求項１８】前記整数要素の組は、前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であり、

前記p_i（ｉ＝１，２，…，ｋ′）を同一の正整数ｐとして、

5

【請求項１９】所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能なｋ′個の成分符号のうちのｋ個の組み合わせが利用者識別番号を一意に表現できる成分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、
抽出された各成分符号に分割する符号分割手段と、
分割された各成分符号をそれぞれ復号する成分符号復号手段と、
各成分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、
前記成分符号復号手段は、前記各成分符号をブロックに分割するブロック分割部と、該ブロック毎にブロック内の“１”のビット数を計数する計数部と、該計数部で得られた計数値が第１の閾値を越えているか否かを判定する第１の判定部と、前記計数値が第２の閾値に満たないか否かを判定する第２の判定部と、前記第１の判定部で第１の閾値を越えていると判定された最小のブロックを決定する最小位置決定部と、前記第２の判定部で第２の閾値に満たないと判定された最大のブロックを決定する最大位置決定部とを有し、前記最小位置決定部及び最大値決定部の決定結果を復号結果として出力する埋め込み符号検出装置。

【請求項２０】前記利用者識別番号の割り当て要求に対して、複数の利用者識別番号候補の中から前記結託者の利用者識別番号として誤検出される可能性のより低い一つの候補を選択し、該選択した利用者識別番号を前記利用者を特定する利用者特定情報に対して割り当てる利用者識別番号割り当て手段をさらに具備する請求項２記載の埋め込み符号生成装置。

【請求項２１】前記利用者識別番号割り当て手段は、前記複数の利用者識別番号候補を一つずつシーケンシャルに入力して、該候補について前記結託者の利用者識別番号として誤検出される可能性の高低を判定し、該可能性が低いと判定した利用者識別番号候補が入力された時点で該候補を前記利用者特定情報に対して割り当てる利用者識別番号として決定する請求項２０記載の埋め込み符号生成装置。

【請求項２２】前記利用者識別番号割り当て手段は、前記結託者の利用者識別番号として誤検出される可能性のより低い複数の利用者識別番号を記憶した記憶手段を有し、該記憶手段に記憶された利用者識別番号の中から前記利用者特定情報に対して割り当てる利用者識別番号を選択して読み出す請求項２０記載の埋め込み符号生成装置。

【請求項２３】前記結託者番号計算手段は、前記複数の剰余対から前記結託者の利用者識別番号である可能性を有する少なくとも一つの利用者識別番号候補を生成し、該候補の中から前記結託者の利用者識別番号として誤検出される可能性のより低い少なくとも一つの利用者識別番号を選択し、該選択した利用者識別番号を前記結託者の利用者識別番号として決定する請求項５記載の埋め込み符号検出装置。

6

【請求項２４】前記結託者番号計算手段は、前記複数の剰余対から前記結託者の利用者識別番号である可能性を有する複数の利用者識別番号候補をシーケンシャルに生成して、該候補について前記結託者の利用者識別番号として誤検出される可能性の高低を判定し、該可能性が低いと判定した全ての利用者識別番号を前記結託者の利用者識別番号として決定する請求項５記載の埋め込み符号検出装置。

【請求項２５】前記結託者番号計算手段は、全ての利用者識別番号に対して、全ての前記剰余対中の剰余に対する前記複数の整数を法とする剰余との間の合同式を満足する個数をそれぞれ求め、この数が所定の閾値以上となる利用者識別番号を前記結託者の利用者識別番号候補として生成する請求項２３または２４記載の埋め込み符号検出装置。

【請求項２６】前記結託者番号計算手段は、前記結託者の利用者識別番号として誤検出される可能性のより低い複数の利用者識別番号を記憶した記憶手段を有し、該記憶手段に記憶された利用者識別番号のうち前記複数の剰余対から生成した前記結託者の利用者識別番号である可能性を有する少なくとも一つの利用者識別番号候補に合致した利用者識別番号を前記結託者の利用者識別番号として決定する請求項５記載の埋め込み符号検出装置。

【請求項２７】請求項２に記載の埋め込み符号生成装置によって生成された埋め込み符号を前記コンテンツに透かし情報として埋め込む電子透かし埋め込み装置。

【請求項２８】所定のコンテンツに対して利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置において、
シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、
出力された符号語を前記透かし情報として前記埋め込み対象コンテンツに埋め込む手段とを具備する電子透かし埋め込み装置。

【請求項２９】所定のコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置において、
シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、
出力された符号語と前記コンテンツとの相関値を求める手段と、
前記相関値に基づいて前記コンテンツ中の前記入力された利用者識別番号に対応する符号語の有無を判定する手段とを具備する電子透かし検出装置。

【請求項３０】所定のコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置において、
予め登録された複数の利用者識別番号にそれぞれ対応する、シンプレックス符号を構成する複数の符号語を出力する手段と、
出力された各符号語と前記コンテンツとの各相関値を求める手段と、
求められた各相関値をベクトルとみなして計算されたノルムに基づいて前記コンテンツ中の透かし情報の有無を判定し、透かし情報があると判定した場合に前記相関値に基づいて結託者を特定する手段とを具備する電子透かし検出装置。
【請求項３１】請求項２に記載の埋め込み符号生成装置によって生成された埋め込み符号が透かし情報として埋め込まれたコンテンツを格納した記憶媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ディジタルデータ化された音声、音楽、動画、静止画等のコンテンツに対して透かし情報を埋め込む電子透かし埋め込み装置及び埋め込み済コンテンツから透かし情報を検出する電子透かし検出装置に関する。
【０００２】
【従来の技術】電子透かし(digital watermarking)は、ディジタルデータ化された音声、音楽、動画、静止画等のコンテンツに対して、コンテンツの著作権者や利用者の識別情報、著作権者の権利情報、コンテンツの利用条件、その利用時に必要な秘密情報、コピー制御情報などの情報(これらを透かし情報と呼ぶ)を知覚が容易ではない状態となるように埋め込み、後に必要に応じて透かし情報をコンテンツから検出することによって利用制御、コピー制御を含む著作権保護を行ったり、二次利用の促進を行うための技術である。
【０００３】[電子透かしの要件]不正利用の防止を目的とする場合、電子透かし技術はディジタル著作物に対して通常に施されると想定される各種の操作や意図的な攻撃によって、透かし情報が消失したり改竄されたりしないような性質(ロバスト性)を持つ必要がある。例えば、静止画や動画はそれぞれＪＰＥＧ(Joint Photographic Coding Experts Group)符号化、ＭＰＥＧ(Moving Picture Experts Group)符号化と呼ばれる非可逆圧縮を施されることが多いため、電子透かし技術はこれらの非可逆圧縮に対するロバスト性を持つことが重要な要件となることが通常である。
【０００４】[電子透かしの分類]従来、画像に対する電子透かしの方式は、画素領域利用型と周波数領域利用型に大別することができる。画素領域利用型の電子透かし方式は、画素値を変更することで直接的に透かし情報の埋め込みを行うものである。一方、周波数領域利用型の

電子透かし方式は、直交変換によって、一旦、画素領域から周波数領域へ移り、周波数領域において埋め込みを行った後、再び、逆直交変換によって周波数領域から画素領域に戻るものである。透かし情報は波として埋め込まれることになる。
【０００５】[周波数領域利用型電子透かし方式]周波数領域利用型の電子透かし方式としては、例えば文献[１] Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T., "Secure Spread Spectrum Watermarking for Multimedia", NEC Research Institute, Technical Report 95-10, 1995. (Coxらの方式という)がある。この方式では、埋め込み対象となる周波数成分を非可逆圧縮による影響が小さな低周波数から中間周波数に設定することで非可逆圧縮に対するロバスト性を実現している。
【０００６】[スペクトラム拡散による電子透かし]スペクトラム拡散(spread spectrum)の考えを適用することで非可逆圧縮へのロバスト性を高める方式がある。スペクトラム拡散とは、通信したい信号に必要な帯域に比べて十分大きな帯域中に、情報を広く分散させて伝送する通信方式をいう(文献[２] 山内雪路, "スペクトラム拡散通信", 東京電機大学出版局, 1994.)。伝送路上のノイズに対する耐性が優れている。元のコンテンツを搬送波、透かし情報を希望波、非可逆圧縮による影響を干渉波(ノイズ)とみなすことで、スペクトラム拡散の考えを電子透かし技術へ適用する。スペクトラム拡散による電子透かし方式として、周波数領域における拡散(先の文献[１]参照)が提案されている。
【０００７】[周波数領域における拡散(摂動法)]先の文献[１]の方式では、透かし情報の埋め込みは画素値に対して直交変換を行い、周波数領域において透かし情報を拡散して埋め込む。拡散は、周波数領域において複数の周波数成分の値とある乱数列に従って変化させることによって行う。拡散後、逆直交変換を行う。透かし情報の検出は、画素値に対して直交変換を行い、埋め込みが行われた周波数成分の値を埋め込みに用いられた乱数列の間の相関値によって判定を行う。埋め込まれた透かし情報は、画素領域では、画像(ブロック)全体に分散されているため、各種の操作に対してロバストである。また、透かし情報を埋め込んだ周波数成分が低中間周波数領域にあるならば、低周波数通過フィルタによっても透かし情報が失われにくい。
【０００８】[フィンガープリンティング]電子透かし方式において、コンテンツに透かし情報として利用者ＩＤ(利用者識別番号)を埋め込むことで、そのコンテンツの利用者を特定する情報を埋め込む応用形態が考えられる。このような応用形態は「フィンガープリンティング」と呼ばれ、不法コピーいわゆる海賊版の再配布を抑止する効果が期待できる。
【０００９】[結託攻撃問題]ところが、同じコンテンツに異なる透かし情報が埋め込まれた複数の埋め込み済み

コンテンツが存在する場合、それら複数の埋め込み済コンテンツを利用して透かし情報を改竄、消失させるという行為が考えられる。このような行為は、「結託攻撃(collusion attack)」と呼ばれている。結託攻撃では、複数の埋め込み済みコンテンツの画素値を平均化することで新たなコンテンツを偽造したり、値が異なる画素値や周波数成分値の部分に対して、ランダムに、あるいは、多数決／少数決に従って値を変更する、などのやり方で改変を加える。

【００１０】[結託攻撃に対する従来の対策]従来、結託攻撃に対処する方法として、スペクトラム拡散による方法(先の文献[１]、及び文献[３]山本哲也，渡辺創，嵩忠雄，“すべての結託ユーザを特定可能な電子透かし法”，SCIS'98，10.2.B，1998.)と、符号理論的な方法(文献[４] Boneh，Dan and Shaw，James，“Collusion-Secure Fingerprinting for Digital Data”，CRYPTO'95，452-465，1995.、文献[５]鈴置昌宏，渡辺創，嵩忠雄，“結託攻撃に強い電子透かし法”，SCIS'97，31B，1997.及び文献[６] 吉田淳，岩村恵市，今井秀樹，“画質劣化が少なく結託攻撃に強い電子透かし法”，SCIS'98，10.2.A，1998.)が提案されている。

【００１１】文献[１]の方法によれば、利用者毎にN(０，１)に従う相異なる実乱数列が与えられる。２つの異なる実乱数列の間に相関がないとする。結託攻撃は、画素値を平均化する操作とする。結託によって、検出時の相関値は減衰してしまう。

【００１２】文献[１]では、相関値の代わりに、定義された類似度によって結託の検出を行う。この類似度は、相関値を検出された透かし情報のノルムで除したものとして定義される。結託により電子透かしのノルムも減衰しているので、相関値が減衰しても類似度はさほど減衰しない。これにより結託者全員を特定することができる。ただし、この方法は検出において埋め込み対象であった原画像を必要とし、また結託者特定に時間がかかるのが難点である。

【００１３】文献[３]では、むしろ平均化による結託攻撃の際の相関値の減衰という性質を利用した結託者の特定方法を提案している。結託者間で共通の電子透かしは減衰せず、それ以外の電子透かしは減衰するので、埋め込み時のレベルを保っている電子透かしの組から結託者の組を特定する。全利用者数をｎ、想定する最大の結託者数をｃとすると、$(c+1)(c-1)\log_{c+1} n$オーダの長さの埋め込み符号で結託者を特定することができる。ただし、この方法はスペクトラム拡散法に特有の性質を利用するため、すべての電子透かし方式に適用が可能なわけではない。

【００１４】先の文献[４]には、透かし情報を表現する符号において、すべての結託者の間で共通な値を持つビットは検出不能であるという性質を利用して、検出不能なビットがそのまま残るならば、それ以外のビットを如

何に変更しようとも、結託者以外の利用者の符号を生成することができない符号(c-frameproof符号と呼ばれる)を埋め込み符号として生成し、コンテンツに透かし情報として埋め込む方式が提案されている。

【００１５】この方式では、埋め込み符号として誰のものでもない符号が生成される可能性は残るものの、ある利用者が自らのコンテンツをそのまま再配布した場合(native redistribution)、その利用者は他者の結託によるものであると主張しての否認はできなくなる。

【００１６】結託者の総数に制限が無いn-frameproof符号は、符号サイズがｎとなる。結託者総数が最大ｃであるc-frameproof符号は、符号サイズが$16c^2\log n$(ｃは結託者数、ｎは全利用者数)である。

【００１７】文献[４]ではさらに、２組の結託者のグループがあって、共通部分が空集合の場合、それぞれのグループ内での結託によって生成できる符号(feasible set)の集合間の共通部分も空集合であるような符号(totally c-secure符号)は存在しないということを示している。つまり、結託攻撃によって誰のものでもない符号を生成することができない符号は、厳密には存在しないことを示した。

【００１８】そこで、文献[４]では結託者数がｃ人以内の場合に結託者を誤って指摘する確率がε以下である符号(c-secure code with ε-error)を埋め込み符号として構成した。まず、誤りεを持つn-secure符号Γ(ｎ，$2n^2\log(2n/\varepsilon)$)を構成した。その符号サイズは、$2n^2(n-1)\log(2n/\varepsilon)$である。

【００１９】さらに、それをTraitor Tracingスキーム(文献[７]Chor，B.，Fiat，A. and Naor，M.，“Tracing traitors”，Proceedings of CRYPTO'94，257-270，1994.)と組合せて誤りがε以下のc-secure符号の可能性を示した。この符号の符号サイズは、$O(c^4\log(n/\varepsilon)\log(1/\varepsilon))$である。

【００２０】[Chernoffの限界(Chernoff bound)]文献[７]では、Traitor Tracingスキームにおいて、Chernoffの限界の式を利用して結託者を特定するために必要な利用者固有鍵の数を決定している。先の文献[４]では、その方法を流用して誤りεのn-secure符号やc-secure符号を構成した。平均値ｐの独立なｎ個の確率変数$X_i \in [0，1]$があるとき、これらの和が平均値からずれる確率の限界を与えるのがChernoffの限界である。上端と下端の限界は、それぞれ次式で与えられる。

【００２１】

【数５】

$$\Pr[\sum_{i=1}^{n} X_i - np > n\delta] < \{\exp(\delta/p)/(1+\delta/p)^{1+\delta/p}\}^{np}$$

$$\Pr[\sum_{i=1}^{n} X_i - np < -n\delta] < \{\exp(-\delta/p)/(1-\delta/p)^{1-\delta/p}\}^{np}$$

11

【００２２】さらに、緩い限界として次式が成り立つ。

【００２３】

【数６】

$$\Pr[|\sum_{i=1}^{n} X_i - np| > n\delta] < 2\cdot\exp\{-\delta^2 n/(2p(1-p))\}$$

【００２４】ここで、$0 \leqq \delta < p(1-p)$とする。また、次式が成り立つ。

【００２５】

【数７】

$$\Pr[\sum_{i=1}^{n} X_i - np < -n\delta] < \exp\{-\delta^2 n/(2p^2)\}$$

【００２６】[結託者中の２人のみを指摘する方法]文献[４]で提案されている誤りεのn-secure符号やc-secure符号は、できるだけ多数の結託者を指摘するように設計されていた。利用者を順序集合とみなし、先の文献[４]で示されている$\Gamma_0(n, d)$符号を、結託者の集合の中から最大と最小の２人を特定する符号として利用することもできる。この場合には、より小さな符号サイズで$\Gamma_0(n, d)$符号を構成することが可能である。

【００２７】ここで、$\Gamma_0(n, d)$符号とはｄビットを一単位とする連続した１の列及び０の列で構成される符号であり、このようなｄビットの１の列や０の列を符号数ｎに応じた単位数だけ並べて構成される。従って、この符号では１と０はそれぞれｄビットを単位として連続するように配置され、ｄビット未満の数の１や０が孤立して存在することはない。

【００２８】例えば、ｄ＝３，ｎ＝５とすれば、$\Gamma_0(n, d)$符号である$\Gamma_0(5, 3)$符号は以下のようになる。

１１１　１１１　１１１　１１１
０００　１１１　１１１　１１１
０００　０００　１１１　１１１
０００　０００　０００　１１１
０００　０００　０００　０００

文献[５]では、２つの符号を昇順と降順に重ね合わせた符号を利用し、結託者中の２人を特定するn-secure符号を提案している。この符号の符号サイズは、$2n\log_4(2/\varepsilon) = n\log_2(2/\varepsilon)$となる。文献[６]では、$\Gamma_0(n, d)$符号において$0 < \mathrm{weight}(x \mid_{Bs})$となる最小のS(Smin)と、$\mathrm{weight}(x \mid_{Bs}) < d$となる最大のS(Smax)を求め、SminとSmax＋１を結託者であると指摘するアルゴリズムによって結託者の２人を特定する方法を示した。この符号の場合、誤りεのn-secure符号は、符号サイズが$(n-1)\log_2(2/\varepsilon)$となる。

【００２９】[誤りεの2-secure符号]結託者総数が小さな場合には、埋め込み符号の符号サイズを小さくすることが可能である。先の文献[６]には、結託者総数２人の場合に結託者の両方を指摘する符号であって、その符号サイズが$(3n^{1/2}-1)\log_2(6/\varepsilon)$の埋め込み符号を

12

示している。

【００３０】[結託攻撃耐性の限界]文献[９] Ergun, Funde, Joe Kilian and Ravi Kumar, "A Note on the Limits of Collusion-Resistant Watermarking", EUROCRYPT'99, 140-149, 1999.)は、電子透かし方式の詳細に依存せずに、結託攻撃に対する耐性には限界があることを理論的に示した。その主張は、正しい結託者を指摘する確率を高くしようとすると、誤った利用者を結託者として指摘してしまう確率(偽陽性率)が高くなってしまうというものであった。

【００３１】文献[９]で想定している結託攻撃は、図３８に示すように異なるすかし情報が埋め込まれた複数のコンテンツ(コンテンツ１，コンテンツ２，コンテンツ３)を平均化し、その後、ランダムな擾乱を加えるというものである。Ergun等の観点から、例えば先の文献[４]での議論を捉えなおしてみる。文献[４]における議論では、確率論的なc-secure符号の構成要素として$\Gamma_0(n, d)$符号を用いている。この$\Gamma_0(n, d)$符号は、図３９(ｄ＝３の例)のように(1, 1, 1)と(-1, -1, -1)に符号をとる符号化をｎ重に直積して得られる。

【００３２】この$\Gamma_0(n, d)$符号に対して、文献[９]で想定された結託攻撃を適用すると、平均化によって得られるコンテンツは、(1, 1, 1)と(-1, -1, -1)を結ぶ直線上にある重心に移る。結託攻撃は、さらに、その重心からずれた位置にコンテンツを移す。この場合、結託攻撃後のコンテンツが(1, 1, 1)か(-1, -1, -1)の近傍にある場合には、これは結託攻撃によって変更されていないと判断し、原点付近にある場合には結託攻撃によって変更されたとみなすことになる。

【００３３】この$\Gamma_0(n, d)$符号において、結託者のうち(1, 1, 1)の符号を持つ者の数と(-1, -1, -1)の符号を持つ者の数の間に大きな偏りがある場合、平均化の結果、重心は(1, 1, 1)あるいは(-1, -1, -1)のかなり近くに位置することとなる。その後、ランダムな擾乱を受けるので、一般に、結託者を特定するアルゴリズムは、コンテンツが(1, 1, 1)または(-1, -1, -1)から擾乱によって移ったものか、重心から擾乱によって移ったものかを誤って判断する可能性が高い。つまり、Ergun等自身、彼らの結論がほとんどの電子透かしアルゴリズムに適用されると言明しているが、Boneh等の符号化もErgun等の限界を逃れることはできないといえる。

【００３４】一方、$\Gamma_0(n, d)$符号において、２つの符号間の最大距離はｎｄ、最小距離はｄと幅が大きい(図４０参照)。$\Gamma_0(n, d)$符号は結託攻撃への耐性に重点がおかれいることから、受信空間中に非常にスパースに符号語が配置されているためである。

【００３５】電子透かしアルゴリズムは、コンテンツの品質への影響がないように、符号間の最大距離ｎｄの符号を埋め込む必要がある。電子透かしアルゴリズムが、$\Gamma_0(n, d)$符号をコンテンツ空間へ埋め込み、その埋

め込みが、符号間の距離とコンテンツ間の距離とが比例するような性質を持つ場合、オリジナルのコンテンツと透かし情報を埋め込んだ後のコンテンツとの間の最大距離もｎｄ／２以上となるので、ｎｄが大きな場合には、コンテンツ品質への影響が大きくなる(図４１の埋め込み1)。

【００３６】仮に、これを避けるため、電子透かしアルゴリズムが符号をコンテンツ空間中のオリジナルコンテンツからの距離関係が保たれないような埋め込みによって、すべての符号語がオリジナルコンテンツとほぼ等しい距離にあるようにしたとすると、$\Gamma_0(n, d)$符号がもともと持っていた結託攻撃への耐性の根拠が失われてしまうことになる(図４１の埋込み2)。

【００３７】つまり、Ergun等の限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式を実現することが望ましいと考えられる。

【００３８】(スペクトラム拡散による電子透かしの結託攻撃耐性)一方、スペクトラム拡散による電子透かし方式では、埋め込みの影響がコンテンツ品質に大きな影響を与えないように埋め込み強度が設定される。その上で、埋め込みに用いる擬似乱数列が符号語に対応する。

【００３９】標本値空間と周波数空間の間の直交変換は線形写像なので、攻撃対象の電子透かし方式が空間領域利用型であれ周波数領域利用型であれ、Ergun等の結託攻撃は擬似乱数列を平均化して、さらに擾乱を与えるという操作となる。

【００４０】スペクトラム拡散による電子透かし方式では、符号語である擬似乱数列は相互相関(cross-correlation)がほとんどゼロとなるように選択されることが普通である。従って、ｋ個のコンテンツの平均によって得られるコンテンツは、ある結託者に対応する擬似乱数列との相関が１／ｋに減衰すると考えられる。擬似乱数列間の相互相関が十分小さく、かつ、このｋがあまり大きくなければ、電子透かしの検出において相関値があるあらかじめ定められた閾値を越えるため、結託者を特定することが可能である。

【００４１】前述した文献[1]の方式は、検出においてオリジナルコンテンツを利用することを前提としており、相関値の代わりに類似度(similarity)と呼ばれる量を用いて検出が行われる。類似度は、検出対象コンテンツからオリジナルコンテンツを引いた差分と埋め込みに用いた擬似乱数列の間の相互相関値を差分の自己相関値の平方根で正規化したものである。

【００４２】類似度による検出では、結託攻撃における平均化によって、分子の相関値が１／ｋに減衰するが、分母の差分のノルムも１／ｋに減衰するため、類似度は減衰しないことが期待される。ただし、平均化以外にノイズが加わる場合には、そのノイズの影響は正規化によってかえって大きくなる。

【００４３】文献[１０] Kilian, Joe, F. Thomas Leighton, Lesley R. Matheson, Talal G. Shamoon, Robert E. Tarjan, and Francis Zane, "Resistance of Digital Watermarks to Collusive Attacks", Technical Report TR-585-98, Departmentof Computer Science, Princeton University, 1998. では、統計的な議論によって文献[1]の電子透かし方式が何人までの結託者による結託攻撃に対する耐性を持っているかという理論的考察を行っている。疑似乱数系列はガウシアンノイズを仮定し、結託攻撃は結託者の持つコンテンツからオリジナルコンテンツを統計的に推定することで行うと仮定する。その結果、現実的なパラメータ設定で、数名から十数名の結託者に対する耐性を実現することが可能であるという結論が得られている。

【００４４】また、電子透かしの応用形態によっては、オリジナルコンテンツを用いた検出が行えず、検出対象コンテンツのみから検出を行う必要がある場合がある。その場合には、類似度による検出は行えない。この場合には、許容される結託者の数はさらに小さくなると考えられる。

【００４５】ところで、文献[1]や文献[１０]での議論は、すべて、符号語である擬似乱数列の間の相互相関が十分小さいという前提に基づいている。しかし、一般に擬似乱数列の数が増えてくると、仮にそれをランダムに選択したとしても、偶然に大きな相互相関値を持つ対が生ずる可能性が高くなってくると思われる。

【００４６】いったい、どの程度多くの擬似乱数系列が任意の対の間で相互相関値を小さくできるのか、また、そのような性質を持つ擬似乱数列をどのように選択すれば良いのか、そして、そのようにして選択された擬似乱数列を符号語として、どのような電子透かし方式を実現すれば、結託攻撃に強い方式となるのかが未解決の問題として残されている。

【００４７】この問題も、先に[結託攻撃耐性]の項で述べた文献[9]での限界を意識した上で、結託攻撃に対する耐性の高さとコンテンツの品質への影響の小ささを適切に両立させた符号化による電子透かし方式をどう実現させるかという問題の一つと考えられる。

【００４８】相互相関の小さな２値の擬似ランダムビット列を生成する方法として、Ｍ系列を利用する方法が知られている。Ｍ系列は、線形フィードバックシフトレジスタ(ＬＦＳＲ)の出力として得られる系列のうち、ＬＦＳＲがＧＦ(2)の原始多項式の係数に対応するタップを持つ場合に生成されるものである。Ｍ系列中の１と０をそれぞれ＋１と－１に置き換えると、ＰＮ系列となる。Ｍ系列は、０の出現頻度が１の出現頻度がほぼ等しく(１の出現頻度が一回少ない)、その間の相互相関関数は０のとき値１、０以外のとき－１／Ｌとなる。ここで、Ｌは系列の周期で、レジスタの段数をｎとすると、Ｌ＝2^n-1である。

【００４９】Ｍ系列から得られたＰＮ系列を巡回シフトして得られる系列を符号語として採用すれば、相互相関の小さな符号語が得られる。これらの符号語を電子透かしの埋め込みの際の擬似乱数系列として用いれば良い。この乱数系列は、空間領域利用型と周波数領域利用型の両方のスペクトラム拡散による電子透かしに利用できる。

【００５０】周波数領域利用型のスペクトラム拡散の電子透かし方式では、普通、Ｎ(０，１)に従うガウシアンノイズを符号語とする。相互相関が小さな符号語を複数構成するには、逐次乱数列を生成し、それが、それまでに生成したすべての乱数列との相関が小さいことを確認し、仮に、大きな相互相関値を持つ場合には、その乱数列は符号語として採用しないという方法をとる。

【００５１】しかし、この方法では、新たに生成した乱数列がそれまでに生成した乱数列と小さな相互相関であるという保証がないため、せっかく生成した乱数列を捨てなければならないことがあるため処理が無駄である。特に、乱数列の数がある程度以上増えると、その確率は高くなる。

【００５２】

【発明が解決しようとする課題】以上に説明したように、従来の電子透かし技術では、結託攻撃によって透かし情報が失われたり偽造されたりすることで、不正な再配布が行われても、その不正行為者を特定できなくなる恐れがあった。

【００５３】また、結託攻撃へのロバスト性を実現する従来の提案において、非常に冗長な形で透かし情報を埋め込む必要があるため、あまり大きな利用者総数や結託者数を想定することができないという欠点があった。大きな利用者総数及び結託者数を想定しても大きな符号サイズの埋め込み符号を透かし情報として埋め込むことは、コンテンツの品質劣化を招く原因となる。

【００５４】さらに、結託者特定の際の埋め込み符号の検出誤りを正しく評価した上で透かし情報(埋め込み符号)を構成する必要があるが、従来の電子透かし技術ではこのような点に対する考察、特に３人以上の結託者が改竄に関与した場合の対策が不十分であり、また検出誤りに対して必要以上に透かし情報である埋め込み符号の符号サイズを大きくしてしまう可能性があった。

【００５５】本発明の目的は、結託攻撃への耐性を有し、利用者総数や結託者総数が大きな場合においても、コンテンツの品質劣化を極力抑えて透かし情報を埋め込む電子透かし埋め込み装置及び電子透かし検出装置と、これらに用いられる埋め込み符号生成方法及び装置、埋め込み符号検出方法及び装置を提供することにある。

【００５６】本発明の他の目的は、結託攻撃への耐性を有し、かつ３人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその

埋め込み符号を正しく検出して復号する埋め込み符号検出方法及び装置を提供することにある。

【００５７】

【課題を解決するための手段】上記の課題を解決するため、本発明に係る第１の埋め込み符号生成装置は、所定のコンテンツに埋め込まれるべき埋め込み符号を生成する埋め込み符号生成装置において、前記コンテンツを利用する利用者の利用者識別番号に対して、互いに素の関係にある複数の整数を法とする複数の剰余を計算する剰余計算手段と、前記剰余計算手段により求められた各剰余を表す複数の成分符号（例えば、所定のビット数を一単位とする連続した１の列及び０の列で構成される符号）を生成する成分符号生成手段と、前記成分符号生成手段により生成された各成分符号を連接して前記埋め込み符号を生成する連接手段とを具備することを特徴とする。

【００５８】この第１の埋め込み符号生成装置においては、前記利用者識別番号の割り当て要求に対して、複数の利用者識別番号候補の中から前記結託者の利用者識別番号として誤検出される可能性のより低い一つの候補を選択し、該選択した利用者識別番号を前記利用者を特定する利用者特定情報に対して割り当てる利用者識別番号割り当て手段をさらに具備してもよい。

【００５９】前記利用者識別番号割り当て手段は、第１の態様によると前記複数の利用者識別番号候補を一つずつシーケンシャルに入力して、該候補について前記結託者の利用者識別番号として誤検出される可能性の高低を判定し、該可能性が低いと判定した利用者識別番号候補が入力された時点で該候補を前記利用者特定情報に対して割り当てる利用者識別番号として決定する特徴とする。

【００６０】請求項２０記載の埋め込み符号生成装置。

【００６１】第２の態様による前記利用者識別番号割り当て手段は、前記結託者の利用者識別番号として誤検出される可能性のより低い複数の利用者識別番号を記憶した記憶手段を有し、該記憶手段に記憶された利用者識別番号の中から前記利用者特定情報に対して割り当てる利用者識別番号を選択して読み出すことを特徴とする。

【００６２】第１の埋め込み符号生成装置に対応する本発明に係る第１の埋め込み符号検出装置は、所定のコンテンツに埋め込まれた複数の成分符号を連接した埋め込み符号を検出する埋め込み符号検出装置において、前記埋め込み符号を前記複数の成分符号に分割する符号分割手段と、分割された各成分符号をそれぞれ復号して予め定められた互いに素の関係にある複数の整数を法とする２つの剰余からなる複数の剰余対を得る成分符号復号手段と、前記複数の剰余対から前記コンテンツに対して結託攻撃を行った結託者の利用者識別番号を計算する結託者番号計算手段とを具備することを特徴とする。また、複数の剰余対から結託の有無を判定する結託有無判定手

段をさらに有し、この結託判定手段により結託があると判定されたとき、結託者番号計算手段が結託者の利用者識別番号を計算するようにしてもよい。

【００６３】ここで、前記結託者番号計算手段は、第１の態様によると、入力されたｋ′個の剰余対の各々から一方の剰余を選択してｋ′個の剰余の組（Ｒ１，Ｒ２，…，Ｒｋ′）を生成する剰余選択部と、前記剰余選択部により生成されたｋ′個の剰余の組から選択された相異なるｋ個の剰余（Ｓ１，Ｓ２，…，Ｓｋ）から中国剰余定理に従って結託者の利用者識別番号ｕの候補を計算する中国剰余定理部と、前記剰余選択部により生成されたｋ′個の剰余の組から前記ｋ個の剰余を選択して前記中国剰余定理部に渡し、前記中国剰余定理部により計算された結託者の利用者識別番号候補ｕの候補から該結託者の利用者識別番号を特定して出力する一貫性検査部とを含み、前記一貫性検査部は、前記剰余選択部により生成されたｋ′個の剰余の組から前記ｋ個の剰余を選択する選択処理と、前記中国剰余定理部により計算された結託者の利用者識別番号ｕの候補と残りの（ｋ′－ｋ）個の剰余のうちの所定個数（ｙ）の剰余との間に$Ri=u \bmod p_{i}$（$i=i_1, i_2, \cdots, i_z$）の関係が成立するか否かを判定する判定処理と、該判定処理により前記関係が成立する場合に結託者の利用者識別番号として出力する出力処理とを有し、前記関係が成立しない場合には前記剰余選択部により生成されたｋ′個の剰余の組から前記選択処理により新たな組み合わせのｋ個の剰余（Ｓ１，Ｓ２，…，Ｓｋ）を選択して前記判定処理を行い、全ての組み合わせのｋ個の剰余（Ｓ１，Ｓ２，…，Ｓｋ）に対して前記関係が成立しない場合には前記剰余選択部に対して新たなｋ′個の剰余の組を要求して、前記関係が成立するまで前記選択処理及び判定処理を繰り返すことを特徴とする。

【００６４】第２の態様による前記結託者番号計算手段は、前記複数の剰余対から前記結託者の利用者識別番号である可能性を有する少なくとも一つの利用者識別番号候補を生成し、該候補の中から前記結託者の利用者識別番号として誤検出される可能性のより低い少なくとも一つの利用者識別番号を選択し、該選択した利用者識別番号を前記結託者の利用者識別番号として決定することを特徴とする。

【００６５】第３の態様による前記結託者番号計算手段*は、前記複数の剰余対から前記結託者の利用者識別番号である可能性を有する複数の利用者識別番号候補をシーケンシャルに生成して、該候補について前記結託者の利用者識別番号として誤検出される可能性の高低を判定し、該可能性が低いと判定した全ての利用者識別番号を前記結託者の利用者識別番号として決定することを特徴とする

また、第２及び第３の態様による前記結託者番号計算手段において、全ての利用者識別番号に対して、全ての前記剰余対中の剰余に対する前記複数の整数を法とする剰余との間の合同式を満足する個数をそれぞれ求め、この数が所定の閾値以上となる利用者識別番号を前記結託者の利用者識別番号候補として生成することを特徴とする第４の態様による前記結託者番号計算手段は、前記結託者の利用者識別番号として誤検出される可能性のより低い複数の利用者識別番号を記憶した記憶手段を有し、該記憶手段に記憶された利用者識別番号のうち前記複数の剰余対から生成した前記結託者の利用者識別番号である可能性を有する少なくとも一つの利用者識別番号候補に合致した利用者識別番号を前記結託者の利用者識別番号として決定することを特徴とする

本発明に係る第２の埋め込み符号生成装置は、入力された利用者識別番号に対応して複数の整数要素の組を計算する計算手段と、所定個数の利用者識別番号に対して前記計算手段により計算される全ての整数要素の組を表現可能なｋ′個の成分符号のうちのｋ個の組み合わせが前記利用者識別番号を一意に表現できる成分符号を前記各整数要素に対応してそれぞれ生成する成分符号生成手段と、この成分符号生成手段により生成された各成分符号を連接して埋め込み符号を生成する連接手段とを具備し、前記ｋ′は、３以上の正整数をｃ、１以上の正整数をｚ、前記埋め込み符号の検出時に前記各成分符号から検出できる前記整数要素の個数をｑとして、ｃ（ｋ＋ｚ）／ｑ以上となるように決定されていることを特徴とし、より好ましくは前記所定個数の利用者識別番号に対して前記計算手段により計算される各整数要素のとり得る値をp_i（ｉ＝１，２，…，ｋ′）とし、前記埋め込み符号の検出時に想定される検出誤り率をεとしたとき、前記ｋ′は、

【００６６】

【数８】

$$\left[1-\prod_{i=1}^{z}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{c(k+z)/2^{Ci+z}2^{k+z}} \geq 1-\frac{\varepsilon}{2} \qquad (1)$$

【００６７】の条件を満たすように設定されていることを特徴とする。

【００６８】ここで、前記計算手段は、例えば入力された利用者識別番号に対応して互いに素の関係にある複数の整数を法とする剰余の組を前記整数要素の組として計算するか、あるいは入力された利用者識別番号に対応して平行移動によって定義される同値類に属する要素の番号の組を前記整数要素の組として計算する。後者の場

19

合、式(1)の条件に加え、前記p_i(i＝1，2，…，k′)を同一の正整数pとして、

$$k' = \frac{c}{2}(k+z) \leq \frac{p^k - 1}{p-1} \quad (2)$$

【００７０】の条件をさらに満たすことを特徴とする。

【００７１】第２の埋め込み符号生成装置に対応する本発明に係る第２の埋め込み符号検出装置は、所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能なk′個の成分符号のうちのk個の組み合わせが利用者識別番号を一意に表現できる成分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各成分符号に分割する符号分割手段と、分割された各成分符号をそれぞれ復号する成分符号復号手段と、各成分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、前記k′は、３以上の正整数をc、１以上の正整数をz、前記埋め込み符号の検出時に前記各成分符号から検出できる前記整数要素の個数をqとして、c(k＋z)／q以上となるように決定されていることを特徴とし、より好ましくは前記所定個数の利用者識別番号に対して計算される各整数要素のとりうる値をp_i(i＝1，2，…，k′)とし、前記埋め込み符号の検出時に想定される検出誤り率をεとしたとき、前記k′は、式(1)の条件を満たすように設定されていることを特徴とする。

【００７２】ここで、前記整数要素の組は、例えば前記利用者識別番号に対応して計算された互いに素の関係にある複数の整数を法とする剰余の組、あるいは前記利用者識別番号に対応して計算された平行移動によって定義される同値類に属する要素の番号の組であり、後者の場合、式(1)の条件に加え、前記p_i(i＝1，2，…，k′)を同一の正整数pとして、式(2)の条件をさらに満たすことを特徴とする。

【００７３】本発明に係る第３の埋め込み符号検出装置は、所定個数の利用者識別番号に対して計算される全ての整数要素の組を表現可能なk′個の成分符号のうちのk個の組み合わせが利用者識別番号を一意に表現できる成分符号であって、入力された利用者識別番号に対応して計算された整数要素の組に対応して生成された部分を連接した埋め込み符号が埋め込まれた対象から該埋め込み符号を抽出する符号抽出手段と、抽出された各成分符号に分割する符号分割手段と、分割された各成分符号をそれぞれ復号する成分符号復号手段と、各成分符号の復号結果から結託者の利用者識別番号を計算する結託者番号計算手段とを具備し、前記成分符号復号手段は、前記各成分符号をブロックに分割するブロック分割部と、該ブロック毎にブロック内の“１”のビット数を計数する計数部と、該計数部で得られた計数値が第１の閾値を越えているか否かを判定する第１の判定部と、前記計数値が第２の閾値に満たないか否かを判定する第２の判定部と、前記第１の判定部で第１の閾値を越えていると判定された最小のブロックを決定する最小位置決定部と、前記第２の判定部で第２の閾値に満たないと判定された最大のブロックを決定する最大位置決定部とを有し、前記最小位置決定部及び最大値決定部の決定結果を復号結果として出力することを特徴とする。

20

【００７４】さらに、本発明によると上述した第１または第２の埋め込み符号生成装置によって生成された埋め込み符号を埋め込み対象コンテンツに透かし情報として埋め込む電子透かし埋め込み装置が提供される。

【００７５】本発明に係る他の電子透かし埋め込み装置は、埋め込み対象コンテンツに対して利用者識別番号の情報を含む透かし情報を埋め込む電子透かし埋め込み装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語を透かし情報として埋め込み対象コンテンツに埋め込む手段とを具備することを特徴とする。

【００７６】本発明に係る他の電子透かし検出装置は、入力されたコンテンツから利用者識別番号の情報を含む透かし情報を検出する電子透かし検出装置であって、シンプレックス符号を構成する複数の符号語から、入力された利用者識別番号に対応して選択された一つの符号語を出力する手段と、出力された符号語とコンテンツとの相関値を求める手段と、この相関値に基づいてコンテンツ中の入力された利用者識別番号に対応する符号語の有無を判定する手段とを具備することを特徴とする。

【００７７】このような本発明に基づく埋め込み符号生成装置／埋め込み符号復号装置及び電子透かし埋め込み／検出装置においては、透かし情報である埋め込み符号の符号サイズを大きくすることなく、利用者総数や結託者数が大きくなっても、結託攻撃に対するロバスト性を得ることができる。

【００７８】また、k′≧c(k＋z)／q以上という条件、さらには式(1)や式(2)の条件を満たすようにすることによって、３人以上の結託者が改竄に関与した場合においても、埋め込み符号検出時の正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号復号装置が実現される。

【００７９】

【発明の実施の形態】図１は、本発明の電子透かし埋め

込み装置１と電子透かし検出装置２が適用されるシステムの例であるフィンガープリンティングシステムの概念図を示す。画像や音声などの埋め込み対象コンテンツと利用者識別番号(以下、利用者識別番号を利用者ＩＤという)が電子透かし埋め込み装置１に入力され、ここで得られた埋め込み済みコンテンツがこれを格納する記憶媒体を含む流通経路３を経て流通する。

【００８０】前述した結託攻撃は、流通経路３において埋め込みコンテンツに対して行われる。このような結託攻撃に対抗するために、本発明に基づく電子透かし検出装置２では、結託の有無を示す結託判定信号、結託があった場合の結託者を特定する結託者ＩＤ(結託者の利用者ＩＤ)、及び結託がなかった場合の正規の利用者ＩＤが生成される。

【００８１】以下、本発明による電子透かし埋め込み装置及び電子透かし検出装置の実施形態について説明する。

(第１の実施形態)本発明の第１の実施形態として、従来例よりも小さな符号サイズを持つε誤りのc-secure符号を埋め込み符号とする電子透かし埋め込み装置及び電子透かし検出装置について説明する。図２(a)(b)は、本発明の第１の実施形態に係る電子透かし埋め込み装置及び電子透かし検出装置の概略構成を示している。図２(a)に示す電子透かし埋め込み装置は、埋め込むべき透かし情報である利用者ＩＤの埋め込み符号を生成する埋め込み符号生成部１１と、生成された埋め込み符号を埋め込み対象コンテンツに埋め込み、埋め込み済みコンテンツを得る符号埋め込み部１２とから構成される。一方、図２(b)に示す電子透かし検出装置は、検出対象コンテンツ(例えば、埋め込み済みコンテンツ)から埋め込み符号を抽出する埋め込み符号抽出部１３と、抽出された埋め込み符号を検出して復号する埋め込み符号検出部１４とから構成される。

【００８２】図３は、埋め込み符号生成部１１の構成を示している。この埋め込み符号生成部１１は、それぞれｋ′個の法記憶部２１－１，２１－２，…，２１－ｋ′、剰余計算部２２－１，２２－２，…，２２－ｋ′、成分符号生成部２４－１，２４－２，…，２４－ｋ′と、符号パラメータ記憶部２３及び符号連接部２５からなる。

【００８３】法記憶部２１－１，２１－２，…，２１－ｋ′には、互いに素の関係にある整数、この例では相異なるｋ′個の素数p_i(ｉ＝１，２，…，ｋ′)が記憶されており、これらの素数p_iが剰余計算部２２－１，２２－２，…，２２－ｋ′に法として供給される。剰余計算部２２－１，２２－２，…，２２－ｋ′は、入力される利用者ＩＤｕに対して、素数p_iを法とする剰余u_i＝ｕ mod p_i(ｉ＝１，２，…，ｋ′)をそれぞれ求める。すなわち、入力された利用者ＩＤに対応した複数の整数要素の組として、剰余計算部２２－１，２２－２，…，２２－ｋ′により剰余u_i＝ｕ mod p_i(ｉ＝１，２，…，ｋ′)が計算される。

【００８４】成分符号生成部２４－１，２４－２，…，２４－ｋ′は、ｋ′個の素数p_i(ｉ＝１，２，…，ｋ′)に対して、符号パラメータ記憶部２３に記憶された符号パラメータｔに従って剰余計算部２２－１，２２－２，…，２２－ｋ′により求められた剰余u_i(ｉ＝１，２，…，ｋ′)を表す前述した$\Gamma_0(n, d)$符号からなる成分符号$\Gamma_0(p_i, t)$をそれぞれ生成する。すなわち、成分符号生成部２４－１，２４－２，…，２４－ｋ′では、所定個数(ｎ)の利用者ＩＤに対して剰余計算部２２－１，２２－２，…，２２－ｋ′で計算される全ての剰余u_i(ｉ＝１，２，…，ｋ′)の組を表現可能なｋ′個の成分符号のうちのｋ個の組み合わせが利用者ＩＤを一意に表現できる成分符号$\Gamma_0(p_i, t)$を各剰余に対応して生成する。

【００８５】符号連接部２５は、成分符号生成部２４－１，２４－２，…，２４－ｋ′により生成された各成分符号$\Gamma_0(p_i, t)$を連接することによって、透かし情報である埋め込み符号を生成する。

【００８６】図４に、成分符号生成部２４－１，２４－２，…，２４－ｋ′の一つ(２４－ｉ)の構成を示す。符号パラメータをｔ、剰余をu_i、法をp_iとすると、減算部３１ではp_i-u_i-1が求められる。“０”列生成部３２では、符号パラメータｔと剰余u_iに基づきｔ×u_iビットの連続した“０”列が生成され、“１”列生成部３３では、符号パラメータｔと減算部３１からの出力p_i-u_i-1に基づきｔ×(p_i-u_i-1)ビットの連続した“１”列が生成される。そして、これらの“０”列と“１”列が連接部３４で連接され、ｔ×(p_i-1)ビットのビット列が$\Gamma_0(n, d)$符号からなる成分符号$\Gamma_0(p_i, t)$として生成される。

【００８７】図５は、こうして生成される成分符号の一例を示している。０からｎ－１までのｎ個の利用者ＩＤに対応して、Ｂ(０)，…，Ｂ(ｎ－２)のブロック“０”列からなる成分符号が割り当てられている。

【００８８】図６に、図２(b)における埋め込み符号検出部１４の構成を示す。この埋め込み符号検出部１４は、検出対象コンテンツから図２(b)の埋め込み符号抽出部１３で抽出された埋め込み符号を入力とする符号分割部４１、成分符号復号部４２－１，４２－２，…，４２－ｋ′、利用者ＩＤ計算部４３、結託判定部４４－１，４４－２，…，４４－ｋ′、結託判定ＯＲ部４５及び結託者ＩＤ計算部４６から構成されている。

【００８９】検出対象コンテンツから埋め込み符号抽出部１３により抽出された透かし情報である埋め込み符号は、符号分割部４１により各成分符号に分割された後、成分符号復号部４２－１，４２－２，…，４２－ｋ′により復号されることにより、利用者ＩＤに対応する剰余対が生成される。

【００９０】こうして生成された各剰余対の一方の剰余から、利用者ＩＤ計算部４３により利用者ＩＤが計算で求められ、また各剰余対から結託判定部４４－１，４４－２，…，４４－ｋ′により結託の有無が判定される。結託判定部４４－１，４４－２，…，４４－ｋ′の判定結果について、結託判定ＯＲ部４５で論理和がとられることにより、結託が存在したか否かが最終的に判定される。さらに、結託が存在すると判定されたときは各剰余対から結託者ＩＤ計算部４６で結託者ＩＤが計算され、結託者が特定される。

【００９１】図７に、結託者ＩＤ計算部４６の詳細な構成を示す。この結託者ＩＤ計算部４６は、ｋ′個の剰余対から各一つの剰余を選択する剰余選択部５１、選択されたｋ′個の剰余のうちｋ個の剰余を選択する一貫性検査部５２、及び一貫性検査部５２で選択されたｋ個の剰余に対して中国剰余定理を適用して結託者ＩＤ候補を得る中国剰余定理部５３からなる。

【００９２】図８に、図７中の一貫性検査部５２の内部構成を示す。中国剰余定理部５３により得られた結託者ＩＤ候補は一貫性検査部５２にフィードバックされ、ｋ′個の剰余のうち残りの(ｋ′－ｋ)個の剰余との間の一貫性検査が行われて、最終的に結託者ＩＤが求められる。図８の一貫性検査部５２は、剰余の(ｋ＋ｚ)組の生成部５２１と、剰余のｚ組と結託者ＩＤ候補の一貫性検査部５２２から構成される。その動作については、後に説明する。

【００９３】本実施形態の電子透かし埋め込み装置及び電子透かし検出装置によると、利用者総数や結託者総数が大きい場合においても、コンテンツの品質劣化の少ない電子透かしが可能となる。以下、詳細に説明する。利用者総数をｎとし、結託者総数の最大値をｃとする。一方、図３の法記憶部２１－１，２１－２，…，２１－ｋ′で用意されているｋ′個の素数ｐ1, p2, …, pk′から任意のｋ個の素数を選んだとき、それらのｋ個の素数の積はｎ以上とする。例えば、この積は$n \leq p_1 \times p_2 \times \cdots \times p_k$である。

【００９４】埋め込み符号生成部１２では、各素数p_i(ｉ＝１，２，…ｋ′)に対して、図３の成分符号生成部２４－１，２４－２，…，２４－ｋ′により成分符号$\Gamma_0(p_i, t)$が生成される。これらの成分符号$\Gamma_0(p_i, t)$を符号連接部２５により連接することによって、新たな符号$\Gamma(p_1, p_2, \cdots, p_{k'}: n, t)$が生成される。

【００９５】ここで、各利用者の利用者ＩＤをｕとすると、その利用者ＩＤｕに対応する連接符号$\Gamma(p_1, p_2, \cdots, p_{k'}: n, t)$の符号語は、各成分符号$\Gamma_0(p_i, t)$がその利用者ＩＤｕに対する素数$p_i$を法とする、剰余計算部２２－１，２２－２，…，２２－ｋ′で計算された剰余$u \bmod p_i$を表す符号語となり、これが透かし情報(埋め込み符号)として埋め込み対象コンテンツに埋め込まれることになる。

【００９６】このようにして得られた埋め込み済みコンテンツに対して結託攻撃が行われた場合、図６の電子透かし検出装置において、符号分割部４１で分割された各成分符号$\Gamma_0(p_i, t)$を成分符号復号部４２－１，４２－２，…，４２－ｋ′で復号することによって、ｃ人中のある２人の利用者ＩＤのp_iに関する剰余(residue)の対が得られる。これをp_iに関する剰余対(residue pair)と呼ぶことにする。

【００９７】また、p_iに関する剰余対中のある剰余がある利用者ＩＤｕを保有する結託者の剰余であるとき、その剰余は利用者ＩＤｕを保有する結託者に起因すると呼ぶことにする。このとき、この結託者を含めて結託者と同じ剰余の値を持つ利用者に関しては、その剰余はその利用者の利用者ＩＤに起因する可能性があると呼ぶことにする。

【００９８】(中国剰余定理(Chinese Remainder Theorem))相異なるｋ個の素数$p_1, p_2, \cdots, p_k$が与えられたとき、各ｉ(ｉ＝１，２，…，ｋ)について$u_i \in Z_{pi}$が与えられると、$u_i \equiv u \bmod p_i$である$u \in Z_{p1} \times Z_{p2} \times \cdots \times Z_{pk}$が一意に定まり、帰納的に計算できる。これが中国剰余定理である。

【００９９】中国剰余定理を適用すると、図７に示すように中国剰余定理部５３にｋ′個の素数のうちｋ個の素数に対応する剰余が与えられれば、それから利用者ＩＤを一意に定めることができる。しかし、それらの剰余すべてが同一結託者の利用者ＩＤに起因するとは限らないため、求めた利用者ＩＤが結託者を正しく特定するとは限らない。

【０１００】そこで、さらに余分にｚ個の剰余を用意し、(ｋ＋ｚ)個の剰余の間の一貫性を検査することで、得られた利用者ＩＤの正当性を検証する。言い換えると、(ｋ＋ｚ)個の連立合同方程式の解の存在を確認する。例えば、ｋ個の剰余から得られた利用者ＩＤに対して、残りの剰余$r_{k+1}, \cdots, r_{k+z}$に対応する整数$p_{k+1}, \cdots, p_{k+z}$で除した余り(remainder)を求め、それらがそれぞれ剰余$r_{k+1}, \cdots, r_{k+z}$に一致し、一致したか否かで結託者を判定することとする。

【０１０１】すなわち、図７の一貫性検査部５２では図８に示すように、図７の剰余選択部５１でｋ′個の剰余対から各一つ選択されたｋ′＝ｃ(ｋ＋ｚ)／２個の剰余を剰余の(ｋ＋ｚ)組の生成部５２１に入力し、これらｋ′個の剰余の中からｋ個の剰余を選択して中国剰余定理部５３に引き渡す。さらに、一貫性検査部５２２により剰余のｚ組と結託者ＩＤ候補との一貫性検査を行って、結託者ＩＤ(結託者の利用者ＩＤ)を出力する。

【０１０２】結託者数が２人の場合については、この方法を比較的容易に実現できる(例えば、特願平１０－１０８０３９，特願平１０－１２２１０８)。ここでは、それを一般の結託者数に拡張する。

25

【０１０３】利用者総数をｎとし、結託者の最大数をｃとする。先の文献[１３]によって導入されたε誤りを持つn-secure符号(cubic length n-secure code with ε-error)は、以下のように定義される。

【０１０４】(定義１)　((ｎ－１)ｄ，ｎ)符号$\Gamma_0(n, *$ｄ)は、その符号語$w^{(0)}, \cdots, w^{(n-1)}$が次の条件を満たす符号と定義する。

$$w^{(i)}|_{B_j} = \begin{cases} \{0\}^d & \text{for } i > j \\ \{1\}^d & \text{otherwise} \end{cases} \quad (3)$$

【０１０５】

【０１０６】ここで、$w^{(i)}|_{Bj}$は符号語$w^{(i)}$をビット位置の集合Ｂｊ に制限したものである。集合Ｂｉ，　ｉ＝０，…，ｎ－２はブロック(blocks)と呼ばれ、ｄ個のビット位置から構成される。異なるブロック間は共通部分を持たない(ｉ≠ｊに対してＢｉ∩Ｂｊ＝φ)。

【０１０７】すべての利用者に対して、シリアル番号のような形で順序をつけることができると仮定する。ｉ番目の利用者に対して、符号語$w^{(i)}$を割り当てるとする。さらに、利用者は自分に割り当てられたシリアル番号を知らされていないとする。

【０１０８】先の文献[１２][１４]によって導入されたε誤りを持つ線形n-secure符号(linear length n-secure code with ε-error)は、符号語は定義１で定義された符号と同一であるが、検出アルゴリズムが異なる。この符号は、結託者中で最大と最小のシリアル番号をもつ２人の結託者を特定することができる。符号サイズは、$\Theta(n)$である。

【０１０９】(定理１)　以下の検出アルゴリズム１を符号$\Gamma_0(n, d)$に適用するとする。ｄ＝$\log_2(2/\varepsilon)$ならば、この符号はε誤りを持ったn-secure符号である。

【０１１０】(検出アルゴリズム１)
(１)検出された符号ｘ∈｛０，１｝^{z}を入力する。ここで、ｚ＝(ｎ－１)ｄ、ｄ＝log(１／ε)とする。
(２)ｓ＝０からｎ－２まで、以下を実行する：
(２－１)もし、$x|_{Bs} \neq \{0\}^d$ならば中断する。
(３)ｔ＝ｎ－２からＳまで、以下を実行する：
(３－１)もし、$x|_{Bt-1} \neq \{0\}^d$ならば中断する。
(４)ｓとｔを出力する。

【０１１１】次に、本発明に特有のアルゴリズム部分について説明する。ｋ，ｋ′，ｚは、ｋ′＝ｃ(ｋ＋ｚ)／２を満足する正整数とする。$p_1, \cdots, p_{k'}$は、互いに素の関係にある整数とする。ｐは$p_1, \cdots, p_{k'}$のうち最小のものとする。また、$p_1, \cdots, p_{k'}$のうち小さい方から選んだｋ個の積をｎ以上とする。これらの整数$p_1, \cdots, p_{k'}$を以下では因数と呼ぶことにする。

【０１１２】これらの因数の平均値をp_{ave}とする($p_{ave} = p_1 + \cdots + p_{k'})/k'$)。ｉ＝１，…，ｋ′の各$p_i$に対応して、先の文献[１３]のn-secure符号$\Gamma_0(p_i, t)$を構成要素の符号として用意する。

【０１１３】(定義２)　((ｐ$_{ave}$－１)ｋ′ ｔ，ｎ)符号$\Gamma(p_1 \cdots, p_{k'}; n, t)$は、その符号語$W^{(1)}, \cdots, W^{(n)}$が

26

次のように構成された符号であると定義する。

$W^{(u)}|_{Ci} = w^{(u \bmod pi)} \in \Gamma_0(p_i, t)$

ここで、Ｃｉは構成要素の符号$\Gamma_0(p_i, t)$に対応するビット位置の集合である。この符号をｕ番目の利用者に割り当てることにする。

【０１１４】埋め込み符号生成のための符号化アルゴリズムは、次の通りである。
(符号化アルゴリズム)
(１)利用者ＩＤｕ∈｛０，…，ｎ－１｝を入力する。
(２)ｉ＝１からｋ′まで以下を実行する：
(２－１)ｕ mod p_iを計算し、符号語$w(u \bmod p_i) \in \Gamma_0(p_i, t)$を生成する。
(３)生成された符号語を連接して、一つの符号語$W^{(u)}$とする。
この符号化アルゴリズムにより生成された埋め込み符号の検出アルゴリズムとしては、先の検出アルゴリズム１を利用する。

【０１１５】(定義３)　$\Gamma(p_1, \cdots, p_{k'}; n, t)$の構成要素に対して、検出アルゴリズム１を適用することで、高々２つの整数$r_i^{(-)}, r_i^{(+)} \in Z_{pi}$を得る。ここで、$0 \leqq r_i^{(-)} \leqq r_i^{(+)} \leqq p_i$である。これらの整数$r_i^{(-)}, r_i^{(+)} \in Z_{pi}$を$\Gamma_0(p_i, t)$の剰余(residues)と呼ぶことにする。また、集合$\{r_i^{(-)}, r_i^{(+)}\}$を$\Gamma_0(p_i, t)$の剰余対(residue pair)と呼ぶことにする。

【０１１６】(定義４)　ｒを$\Gamma_0(p_i, t)$の剰余とする。結託者の集合の中にｒ≡ｕ mod p_iを満たす結託者が存在する場合、剰余ｒはｕに起因する(r arises from u)と呼ぶ。また、利用者が結託者であるか否かに関わらず、ｒがｒ≡ｕ mod p_iを満足する場合、剰余ｒはｕに起因する可能性がある(possibly arise from)と呼ぶ。

【０１１７】(定義５)　ｍ個の素数に対応する剰余の組(m-tuple of residues)の中の任意のｋ個の剰余に対して中国剰余定理を適用したとき、これらｍ個の剰余の組がすべて同一の利用者ＩＤを与える場合、このような剰余の組を一貫している(consistent)と呼ぶことにする。

【０１１８】さらに、このような一貫している剰余の組の全ての剰余が、求められた結託者の利用者ＩＤに起因している場合、この剰余の組は真に一貫している(truly consistent)と呼び、そうでない場合、この剰余の組は偽って一貫している(falselyconsistent)と呼ぶことに

する。このような偽って一貫している組の簡単な例を以下に挙げる。

(検出アルゴリズム２)

(１)検出された符号ｘ∈{０，１}^{L}を入力する。ここで、Ｌ＝(ｐ$_{ave}$－１)ｋ′ ｔとする。

(２)ｘをｋ′ 個の制限ｘ｜$_{Ci}$，ｉ＝１，…，ｋ′ 個に分解する。

(３)ｉ＝１からｋ′ まで以下を実行する：

(３－１)検出アルゴリズム１をｘ｜$_{Ci}$に適用する。

(４)全ての剰余のｍ組に対して以下を実行する：

＊(４－１)もし、剰余のｍ組が一貫しているならば、以下を実行する：

(４－２)その解を結託者として出力し中止する。

(５)結託者が検出されなかったと出力する。

【０１１９】(定理２)　ｔ≧log$_{2}$(４ｋ′ ／ε)とする。以下の方程式が成立するとき、符号Γ(ｐ１，…，ｐｋ′ ；ｎ，ｔ)はε誤りを持ったc-secure符号である。

【０１２０】

【数１１】

$$\left[1-\left\{1-\left(1-\frac{1}{p}\right)^{t}\right\}^{k}\right]^{k\cdot Ck+z\times 2^{k+z}} > 1-\frac{\varepsilon}{2} \qquad (4)$$

【０１２１】このとき、符号サイズは、Ｌ＝(ｐ$_{ave}$－１)ｋ′ ｔで与えられる。

【０１２２】(補題１)　符号Γ(ｐ１，…，ｐｋ′ ；ｎ，ｔ)のｋ′ 個の剰余対の中には、少なくとも２ｋ′ ／ｃ個の剰余を起因させている結託者が少なくとも１人存在する。

(補題１の証明)　符号Γ(ｐ１，…，ｐｋ′ ；ｎ，ｔ)のｋ′ 個の剰余対に含まれる剰余は２ｋ′ 個ある。平均すると、結託者１人あたり２ｋ′ ／ｃ個の剰余を起因させていることになる。従って、少なくとも１人の結託者は、２ｋ′ ／ｃ個以上の剰余を起因させている。

【０１２３】(補題１の一般化)補題１は、各成分符号から検出できる整数要素(剰余)の個数ｑをｑ＝２とした場合の例であるが、これをｑを用いて一般化すると、次の通りとなる。

【０１２４】(一般化した補題１の証明)符号Γ(ｐ$_{１}$，…，ｐ$_{ｋ′}$；ｎ，ｔ)のｋ′ 個の剰余ｑ対(対ではないが、ここでは便宜上、そう呼ぶことにする)に含まれる剰余は、ｑｋ′ 個ある。平均すると結託者１人あたり、ｑｋ′ ／ｃ個の剰余を起因させていることになる。従って、少なくとも１人の結託者は、ｑｋ′ ／ｃ個以上の剰余を起因させている。

【０１２５】ここで、結託者ＩＤ(結託者の利用者ＩＤ)の再構成と検定には、(ｋ＋ｚ)個の剰余が必要なので、一般化した補題１の結果より、ｑｋ′ ／ｃ≧ｋ＋ｚが成立する必要がある。左辺の因子ｑ／ｃを右辺に移すと、条件式ｋ′ ≧ｃ(ｋ＋ｚ)／ｑを得る。実際には、ｋ′ は整数であるので、ｋ′ ≧[ｃ(ｋ＋ｚ)／ｑ]である。

【０１２６】(補題２)　ｔ≧log$_{2}$(２ｋ′ ／ε)とする。※

【０１２７】(補題２の証明)　ある構成要素Γ$_{0}$(ｐ$_{ｉ}$，ｔ)に対して検出アルゴリズム１を適用するときは、定理１よりｔ≧log$_{2}$(２ｋ′ ／ε)ならば、剰余対の検出誤り率はε／ｋ′ 以下である。全部でｋ′ 個の構成要素が存在するので、全ての剰余対に対する検出誤り率はε以下である。

(補題３)　ある一貫した剰余のｍ組が存在しており、これに別の因数ｐに対する剰余対からの剰余を加えて剰余の(ｍ＋１)組を構成するとき、この(ｍ＋１)組の剰余が偽に一貫している確率は、１－(１－１/ｐ)^{c}以下である。

【０１２８】(補題３の証明)　各剰余対は、全ての結託者の利用者ＩＤに対するｑを法とする剰余のうちの最大値と最小値により構成されている。利用者は自分の利用者ＩＤを知らないので、結託が行われたとき、ある利用者ＩＤが結託者のものである確率は、利用者ＩＤによらず一様であると考えられる。従って、ある結託者の剰余がある値をとる確率は、等しく１／ｐである。

【０１２９】ｃ人の結託者の剰余が全て一様に分布するとき、最大の剰余がある値ｃ∈Ｚ／ｐＺをとる確率Ｐｒ[ｘ]は、以下のように与えられる。なお、Ｚ／ｐＺは０以上、ｐ未満の整数の集合である。

【０１３０】

【数１２】

$$Pr[x]=\begin{cases}\left(1-\dfrac{x}{p}\right)^{c}-\left(1-\dfrac{x+1}{p}\right)^{c} & \text{for } x\neq p-1\\ \left(\dfrac{1}{p}\right)^{c} & \text{for } x=p-1\end{cases} \qquad (5)$$

【０１３１】(補題４)　以下の条件が成り立つとき、偽に一貫している剰余の(ｋ＋ｚ)組が存在する確率は次式に示すようにε以下である。

【０１３２】

29 30

【数１３】

$$\left[1-\left\{1-\left(1-\frac{1}{p}\right)^{c}\right\}^{z}\right]^{c(k+z)/2\,Ck+z\times 2^{k+z}} \geq 1-\varepsilon \qquad (6)$$

【０１３３】(補題４の証明)　ｋ′個の剰余対から剰余の(ｋ＋ｚ)組を選択する組合せは、$_{k'}C_{k+z}\times 2^{k+z}$通りある。補題１４から、剰余の(ｋ＋ｚ)組が偽に一貫している確率は、$(1-(1-1/p)^{c})^{z}$である。従って、全ての組合せにおいて、少なくとも1個の偽に一貫＊している剰余の(ｋ＋ｚ)組が現れる確率は、次のような上限が与えられる。

【０１３４】

【数１４】

$$P_F \leq \left[1-\left\{1-\left(1-\frac{1}{p}\right)^{c}\right\}^{z}\right]^{k/2\,Ci+z\times 2^{k+z}} \qquad (7)$$

【０１３５】補題１の条件式が成立するとき、確率P_Fはε以下である。

【０１３６】(定理２の証明)　潔白な利用者を誤って結託者であると検出する原因は、剰余対の検出誤りと、偽に一貫している剰余の組の選択の二つがある。それぞれの確率をε／２以下とするならば、検出誤り率はε以下となる。補題２と補題４より、上の上限の式を得る。偽※に一貫している剰余の組を排除する確率を最小の因数で下限を抑える代わりに、小さい方からｚ個の因数を用いて下限を抑えることで、式(4)に代えて次式(8)に示すような符号サイズのより小さな上限を得ることができる。

【０１３７】

【数１５】

$$\left[1-\prod_{i=1}^{z}\left\{1-\left(1-\frac{1}{p_i}\right)^{c}\right\}\right]^{c(k+z)/2\,Ci+z\times 2^{k+z}} \geq 1-\frac{\varepsilon}{2} \qquad (8)$$

【０１３８】ここで、$p_1, \cdots, p_z$は$p_1, \cdots, p_k'$の中から選んだｚ個(ただし、$p_1<p_2\cdots<p_z$とする)であり、最も小さいものから順に選んだｚ個であってもよいし、ｋ＋ｚ番目から小さい順に最も大きいｋ＋ｚ番目まで選んだｚ個であってもよいし、あるいは最も小さいものからｋ＋ｚ番目に小さいものまでの中から選んだｚ個であってもよい。また、p_i(ｉ＝１，２，…，ｋ′)はｃ個の利用者ＩＤに対して剰余計算部で計算される各剰余(整数要素)のとりうる値であり、本実施形態では前述の法記憶部２１－１，２１－２，…，２１－ｋ′で用意されているｋ′個の素数である。

【０１３９】式(8)の意味について説明する。まず、式(8)の左辺は、検出が正しく結託者ＩＤを特定する確率の下限を与えている。つまり、左辺の大括弧の肩に乗っている「べき」は、ｋ′個の剰余対から(ｋ＋ｚ)個の剰余を選択してくる場合の例である。その個々の選択に対して、結託者ＩＤが正しいか否かの判定を正しく行う確率の加減が右辺全体の意味するところである。

【０１４０】ここで、式(8)左辺の大括弧の中身について詳しく説明する。上記の各選択では、結託者ＩＤが正しいか否かを余分にｚ個の剰余によって検定している。大括弧の中のΠによる積の部分は、ｚ個の検定すべてが、誤った結託者ＩＤを正しいとしてしまう確率の上限を与えている。なぜなら、各検定が誤った結託者ＩＤを正しいと判定してしまう確率の下限は、(補題３)において、与えている確率$1-(1-1/p)^{c}$において、各成分符号から検出できる整数要素(剰余)の個数ｐをその剰余に対応する因数で置き換えたものによって与えられる。

【０１４１】検定に用いられる剰余に対応するｚ個の因数は、最も小さな因数からなる組み合わせが$p_1, p_2, \cdots, p_z$の場合であって、この組み合わせが、誤った検定を行う確率の下限を最大にする組み合わせである。よって、Πによる積部分がｚ個の検定すべてが、誤った結託者ＩＤを正しいとしてしまう確率の上限を与えていることになる。よって、式(8)は左辺であるところの正しい結託者ＩＤを検出する確率の下限が右辺であるところの$1-\varepsilon/2$以上であるための条件式を意味していることになる。このように本実施形態によると、前述した一般化した補題１によって与えられる条件式$k' \geqq (k+z)/q$を満たすように、より好ましくは式(8)を満足するように成分符号の数ｋ′を規定することによって、結託攻撃への耐性を有し、かつ３人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づ

いて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することができる。

【０１４２】次に、本実施形態における結託者を特定するアルゴリズムについて図９に示すフローチャートを用いて説明する。結託者ＩＤ計算部４６は、成分符号復号部４２－１，４２－２，…，４２－ｋ′が出力したｋ′個の剰余対を入力する(ステップＳ１)。剰余対は、まず剰余選択部５１に入力される。剰余選択部５１は、各剰余対から一方の剰余を選択し、ｋ個の剰余の組(R_1, R_2, …, $R_{k'}$)を生成する(ステップＳ２)。

【０１４３】生成されたｋ′個の剰余の組は、一貫性検査部５２に入力される。一貫性検査部５２は、入力されたｋ′個の剰余の組から相異なるｋ個の剰余(S_1, S_2, …, S_k)を選択し(ステップＳ３)、中国剰余定理部５３に渡す。

【０１４４】中国剰余定理部５３は、中国剰余定理に従い結託者ＩＤｕを計算する(ステップＳ４)。この中国剰余定理の計算は、図１０のフローチャートに示す処理の流れに従って行われる。計算された結託者ＩＤｕは、一貫性検査部５２へ返される。

【０１４５】一貫性検査部５２では、残りの(ｋ′－ｋ)個の剰余のうちの所定個数(ｚ)の剰余との間に、$R_i = u \bmod p_i$ ($i = i_1, i_2, \cdots, i_z$)の関係が成立する場合があるか否かを判定する(ステップＳ５)。この関係が成立する場合、一貫性検査部５２はｕを結託者ＩＤとして出力する(ステップＳ６)。この関係が成立しない場合には、この関係が成立するまで、ステップＳ３で入力されたｋ′個の剰余の組から新たな相異なるｋ個の剰余(S_1, S_2, …, S_k)を選択して中国剰余定理部５３に渡す処理を行う。

【０１４６】ステップＳ７でｋ個の剰余(S_1, S_2, …, S_k)が最後の候補と判定されると、一貫性検査部５２は剰余選択部５１に対して新たなｋ′個の剰余の組を要求し(ステップＳ８)、ステップＳ５で$R_i = u \bmod p_i$ ($i_1, i_2, \cdots, i_z$)の関係が成立するまでステップＳ３，Ｓ４，Ｓ７の処理を繰り返す。もし、ステップＳ７で新たなｋ個の剰余(S_1, S_2, …, S_k)の候補が存在しない場合には、結託者ＩＤの特定に失敗したとする(ステップＳ９)。

【０１４７】最後に、図１１に示すフローチャートを用いて本実施形態における埋め込み符号検出部１４の処理の流れについて説明する。検出対象コンテンツ(例えば埋め込み済みコンテンツ)が入力され(ステップＳ１１)、この検出対象コンテンツから埋め込み符号が抽出されると(ステップＳ１２)、符号分割部４１及び部分復号部４２－１，４２－２，…，４２－ｋ′を介して得られた成分符号に基づいて、結託判定部４４－１，４４－２，…，４４－ｋ′により結託の有無が判定される(ステップＳ１３)。

【０１４８】ここで、結託判定部４４－１，４４－２，…，４４－ｋ′のいずれでも結託が無いと判定されると、利用者ＩＤ計算部４３により利用者ＩＤが計算され(ステップＳ１４)、この利用者ＩＤが出力される(ステップＳ１５)。

【０１４９】一方、ステップＳ１３で結託判定部４４－１，４４－２，…，４４－ｋ′の少なくとも一つで結託が有ると判定されると、結託判定部４５を介して結託存在信号が出力され(ステップＳ１６)、かつ結託者ＩＤ計算部４６で結託者ＩＤが計算され(ステップＳ１７)、この結託者ＩＤが出力される(ステップＳ１８)。

【０１５０】この場合、ステップＳ１３での結託の有無の判定と、ステップＳ１４での利用者ＩＤの計算については、処理が簡単であり、高速に行うことができる。これに対して、ステップＳ１７での結託者ＩＤの計算には時間がかかるが、結託の有無の判定を先に行い、結託が有ったと判断された場合にのみ結託者ＩＤの計算を行うことにより、無駄な計算を省略できる。

【０１５１】また、本発明の電子透かし検出装置を利用者機器に適用する場合には、結託の有無のみを判定し、その結果によって利用を中断させるなどの利用制御を行えばよいので、結託者の計算(特定)まで行う必要は必ずしもない。

【０１５２】このように本実施形態によると、埋め込むべき符号サイズを抑えつつ、利用者総数や結託者数が大きい場合についても、結託攻撃に対するロバスト性を持つことができる。

【０１５３】(第２の実施形態)図１２は、本発明の第２の実施形態における埋め込み符号生成部１１の構成を示している。本実施形態の埋め込み符号生成部１１では、図３に示した構成にコンテンツの利用者を特定する利用者特定情報に対して利用者ＩＤを割り当てる利用者ＩＤ割り当て部２６と、利用者ＩＤと利用者ＩＤ割り当て部２６により割り当てられた利用者ＩＤとを対応付けて格納した利用者特定情報／利用者ＩＤ対応テーブル２７が追加されている。

【０１５４】利用者ＩＤ割り当て部２６では、入力された利用者特定情報に対して後述するように利用者ＩＤの割り当てが行われ、この割り当てられた利用者ＩＤが剰余計算部２２－１～２２－ｋ′に入力される。また、利用者特定情報／利用者ＩＤ対応テーブル２７は、図１３に示されるように、利用者ＩＤ割り当て部２６は利用者ＩＤ候補生成部２６１、利用者ＩＤ候補判定部２６２及び利用者ＩＤ決定部２６３から構成される。図１４に示すフローチャートを用いて、図１３の利用者ＩＤ割り当て部２６の処理手順を説明する。

【０１５５】まず、利用者特定情報を入力する(ステップＳ２１)。利用者特定情報は、個々の利用者に対応してユニークな識別情報であり、例えば利用者の氏名が用いられる。利用者特定情報に対応して、利用者ＩＤ候補生成部２６１において利用者ＩＤ候補を一つずつ生成す

33

る(ステップＳ２２)。利用者ＩＤ候補としては、まだ割り当てられていない(使用されていない)ＩＤが用いられる。

【０１５６】次に、各利用者ＩＤ候補について弱ＩＤか否かの判定を利用者ＩＤ候補判定部２６２において順次行う(ステップＳ２３)。弱ＩＤとは、複数の利用者ＩＤ候補のうちで結託者ＩＤでない、つまり無実(結託者でない)の利用者の利用者ＩＤであるにも関わらず、結託者ＩＤとして誤検出される可能性のより高い利用者ＩＤであり、誤検出に弱いＩＤという意味から、このように呼ぶものとする。このステップＳ２３の判定の結果、利用者ＩＤ候補が弱ＩＤである場合は、ステップＳ２２に戻って次の利用者ＩＤ候補を生成し、再びステップＳ２３の判定を行う。

【０１５７】ステップＳ２３の判定の結果、利用者ＩＤ候補が弱ＩＤでなければ、つまり結託者ＩＤとして誤検*

34

*出される可能性のより低い利用者ＩＤ(これを誤検出に弱くないＩＤという意味で、非弱ＩＤという)であれば、利用者ＩＤ候補決定部２６３においてその利用者ＩＤ候補をステップＳ２１で入力された利用者特定情報に割り当てる利用者ＩＤに決定する(ステップＳ２４)。

【０１５８】図１５に示すフローチャートを用いて、利用者ＩＤ候補が弱ＩＤか非弱ＩＤかを判定するステップＳ２３の判定処理の具体的な手順を説明する。まず、ステップＳ２２で生成された利用者ＩＤ候補を一つずつシーケンシャルに入力し(ステップＳ３１)、この利用者ＩＤ候補が結託者ＩＤとして誤検出される確率(誤検出確率)を推定する(ステップＳ３２)。この誤検出確率の推定は、例えば前述したｐi，ｋ，ｋ′，ｃといったパラメータを用いて次のようにして行われる。まず、

【数１６】

$$\Pr[x;p,c]=\begin{cases}\left(1-\dfrac{x}{p}\right)^{c}-\left(1-\dfrac{x+1}{p}\right)^{c} & \text{for } x\neq p-1\\ \left(\dfrac{1}{p}\right)^{c} & \text{for } x=p-1\end{cases} \qquad (9)$$

を定義する。次に、

※ ※【数１７】

$$Q[x;p,c]=\Pr[x;p,c]+\Pr[p-1-x;p,c] \qquad (10)$$

を定義する。ある利用者ＩＤ(ｕとする)が結託者ＩＤとして誤検出される確率を概ね表す量として、次の評価値ＥＥＦを計算する。

★【０１５９】

【数１８】

★

$$EEP=1-\prod_{\substack{\{j(1),j(2),\ldots,j(k+z)\}\subset\{1,2,\ldots,k'\},\\ j(1)<j(2)<\ldots<j(k+z)}}\left\{1-\prod_{j=1,2,\ldots,k+z}Q[u_{pi};p_i,c]\right\} \qquad (11)$$

【０１６０】ここで、ｕp＝ｕ mod ｐとする。これ以外にも、ある利用者ＩＤについて誤検出確率を近似する評価値が存在するならば、それを式(１１)のＥＥＰの代わりに用いることが可能である。例えば、次式(１２)で表☆

☆される評価値ＥＥＰを用いてもよい。

【０１６１】

【数１９】

$$EEP=\sum_{i=0,1,\ldots,k'}Q[u_{pi};p_i,c] \qquad (12)$$

【０１６２】次に、ステップＳ３２で推定された誤検出確率(例えば、式(１１)または(１２)のＥＥＦ)が所定の閾値を超えたか否かを調べ(ステップＳ３３)、閾値を超える場合は、利用者ＩＤ候補が弱ＩＤであると判定し(ステップＳ３４)、また誤検出確率が閾値以下の場合は、利用者ＩＤ候補が非弱ＩＤであると判定する(ステップＳ３５)。

【０１６３】このようにして図１２中に示した利用者ＩＤ割り当て部２６では、入力された利用者特定情報に対して、複数の利用者ＩＤ候補の中から結託者ＩＤとして誤検出されにくいＩＤ(非弱ＩＤ)が利用者ＩＤとして割り当てられる。以後、こうして利用者ＩＤ割り当て部２６で割り当てられた利用者ＩＤに対して、第１の実施形態と同様に剰余計算部２２－１～２２－ｋ′、成分符号生成部２４－１～２４－ｋ′及び符号連接部２５により順次処理が行われることによって、埋め込み符号が生成される。

【０１６４】言い換えれば、利用者ＩＤ割り当て部２６においては、入力された利用者特定情報に対して、複数の利用者ＩＤ候補の中から結託者ＩＤとして誤検出されやすい弱ＩＤを利用者ＩＤに割り当てないようにすることによって、誤検出の確率を小さくすることができる。仮に、弱ＩＤが結託者ＩＤとして検出されたとしても、それは結託者ＩＤとして見なさないことにすればよい。

35

【０１６５】ところで、弱ＩＤは埋め込み符号の符号長の決定に大きな影響を与える。電子透かし検出装置においてある利用者ＩＤが検出されたとき、それがたとえ弱ＩＤであったとしても誤検出確率をある許容される確率より小さくするためには、非常に多数の因数からなる因子基底(具体的には、法記憶部２１－１，２１－２，…，２１－ｋ′に記憶される互いに素の関係にある整数、例えば相異なるｋ′個の素数p_i(ｉ＝１，２，…，ｋ′))を用意する必要がある。しかし、弱ＩＤを排除しない場合に、ある埋め込み符号がある誤検出確率を持つ*場合、弱ＩＤを利用者ＩＤから排除することによって、より少数の因子からなる因子基底を持つ埋め込み符号によって同等の誤検出確率を実現できる。

36

【０１６６】このことは、次のように説明できる。ある利用者ＩＤをｕとし、このｕが検出されるという事象をdetect(u)、ｕが弱ＩＤであるという事象をweak(u)、ｕが結託者ＩＤであるという事象をcollude(u)と表すことにする。このとき、

【数２０】

$$\begin{aligned}\mathrm{detect}(u) = {} & \mathrm{detect}(u) \wedge \mathrm{weak}(u) \wedge \mathrm{collude}(u) \\ & \vee \mathrm{detect}(u) \wedge \mathrm{weak}(u) \wedge \neg\mathrm{collude}(u) \\ & \vee \mathrm{detect}(u) \wedge \neg\mathrm{weak}(u) \wedge \mathrm{collude}(u) \\ & \vee \mathrm{detect}(u) \wedge \neg\mathrm{weak}(u) \wedge \neg\mathrm{collude}(u)\end{aligned} \quad (13)$$

であるから、

※　※【数２１】

$$\begin{aligned}\Pr[\mathrm{detect}(u)] = {} & \Pr[\mathrm{detect}(u) \wedge \mathrm{weak}(u) \wedge \mathrm{collude}(u)] \\ & + \Pr[\mathrm{detect}(u) \wedge \mathrm{weak}(u) \wedge \neg\mathrm{collude}(u)] \\ & + \Pr[\mathrm{detect}(u) \wedge \neg\mathrm{weak}(u) \wedge \mathrm{collude}(u)] \\ & + \Pr[\mathrm{detect}(u) \wedge \neg\mathrm{weak}(u) \wedge \neg\mathrm{collude}(u)]\end{aligned} \quad (14)$$

となる。これらのうち誤検出率に寄与するのは、式(１４)右辺の第２項と第４項である。符号長を短くするには、誤検出率を低下させることなく、より小さな個数(ｋ′)の因数によって結託者ＩＤ候補の検定を行うことができるような方法を採用すればよい。ここで、単純により小さな個数の因数によって結託者ＩＤ候補の検定を行う場合は、式(１４)右辺の第４項の確率はさほど変化しないが、第２項の確率は大きく増加してしまい、誤検出確率が増加してしまう。

【０１６７】しかし、前述したように弱ＩＤを予め利用者ＩＤとして割り当てないように排除しておけば、式(１４)右辺の第２項は誤検出確率には組み込まれない。後述する埋め込み符号検出部１４において結託者ＩＤ候補の利用者ＩＤリストを用意しておき、その利用者ＩＤリストの中から同じＩＤを取り出していけば、やがて非弱ＩＤが得られる確率が高いので、それを結託者ＩＤと決定することにすれば、結果的に短い符号長の埋め込み符号を生成できることになる。

【０１６８】図１６は、第２の実施形態における埋め込み符号検出部１４の構成を示している。本実施形態では、第１の実施形態と同様に図６で説明した符号分割部４１を経て成分符号復号部４２－１，４２－２，…，４２－ｋ′で得られた利用者ＩＤに対応するｋ′個の剰余対が結託者ＩＤ計算部４７に入力される。

【０１６９】結託者ＩＤ計算部４７で計算された結託者ＩＤは、結託者特定情報生成部４９に入力され、この結託者特定情報生成部４８において図１２で説明した利用者特定情報／利用者ＩＤ対応テーブル２７を参照して結託者特定情報が生成される。結託者ＩＤ計算部４７は、図６中に示した結託者ＩＤ計算部４６と異なり、利用者ＩＤを以下のようにして計算する。

【０１７０】図１７に示されるように、結託者ＩＤ計算部４７は結託者ＩＤ候補生成部４７１、結託者ＩＤ候補判定部４７２及び結託者ＩＤ決定部４７３から構成される。以下、図１８に示すフローチャートを用いて、図１７の結託者ＩＤ計算部４７の処理手順を説明する。

【０１７１】まず、結託者ＩＤ候補生成部４７１の処理について説明する。成分符号復号部４２－１，４２－２，…，４２－ｋ′で得られたｋ′個の剰余対を入力する（ステップＳ４１）。次に、既に使用されている全ての利用者ＩＤをｊ（ｊ＝０～ｎ－１）として、まず、ｊ＝０に設定する（ステップＳ４２）。次に、現在設定されているｊが利用者ＩＤの範囲を越えているか（ｊ＞ｎ－１）否か（ｊ≦ｎ－１）を判定する（ステップＳ４３）。ｊが利用者ＩＤの範囲を越えている場合には、結託者ＩＤの計算を終了する。

【０１７２】一方、ｊが結託者ＩＤの範囲を越えていない場合には、その利用者ＩＤ（ｊ）について、図１８のステップＳ４１で入力されたｋ′個の全ての剰余対に対して、いずれかの剰余($r_i^{(+)}$または$r_i^{(-)}$)に対するp_iを法とする合同式$j \equiv r_i^{(\pm)} \bmod p_i$を満足している場合の数ｘを計数する（ステップＳ４４）。以下、この場合の数ｘを「合同式充足数」と呼ぶ。

【０１７３】次に、この合同式充足数（ｘ）が所定の閾値ｙ以上かどうかを調べる（ステップＳ４５）。この閾値ｙの値は、検出誤りを小さくしたい場合には大きな値

を、検出誤りが大きくて良い場合には大きな値をそれぞれ設定することができる。以下で説明するような、結託者ＩＤ候補に対して弱ＩＤか否かによる判定を行う場合には、ｙとしてｋ＋ｚよりも小さな値に設定した場合でも、検出誤りをε以下とできることがある。しかし、そのような判定を行わない場合には、ｙはｋ＋ｚ以上の値に設定しないと、検出誤りをε以下にできない。

【０１７４】合同式充足数ｘがこの閾値ｙ以上の場合には、ｊは結託者ＩＤ候補であると決定する（ステップＳ４６）。一方、ｘが閾値ｙより小さい場合には、後述するステップＳ４９に進む。こうして生成された結託者ＩＤ候補が、結託者ＩＤ候補生成部４７１より出力される。

【０１７５】次に、結託者ＩＤ候補判定部４７２の処理について説明する。結託者ＩＤ候補生成部４７１が生成した結託者ＩＤ候補は、弱ＩＤであって、本当の結託者ＩＤではない恐れがある。そこで、結託者ＩＤ候補判定部４７２は、こうして生成された結託者ＩＤ候補ｊが弱ＩＤであるか否かを判定する（ステップＳ４７）。弱ＩＤとは、前述したように結託者ＩＤでないにもかかわらず、結託者ＩＤとして誤検出される可能性のより高い利用者ＩＤである。一方、結託者ＩＤとして誤検出される可能性のより低い利用者ＩＤを非弱ＩＤと呼ぶ。

【０１７６】最後に、結託者ＩＤ決定部４７３の処理について説明する。結託者ＩＤ候補判定部４７２におけるステップＳ４７の判定の結果、結託者ＩＤ候補が弱ＩＤでなければ、つまり、結託者ＩＤとして誤検出される可能性のより低い利用者ＩＤであれば、結託者ＩＤ決定部４７３によって、その結託者ＩＤ候補を結託者ＩＤに決定する（ステップＳ４８）。一方、ステップＳ４７の判定の結果、結託者ＩＤ候補が弱ＩＤである場合には、ステップＳ４９に進む。

【０１７７】以上は、ｊの一つの値に対して行われる処理である。ステップＳ４９では、次のｊについて同様の処理を行うため、ｊを１だけ増加させる。その後、ステップＳ４３に戻り、同様の処理を繰り返す。従って、図１９の結託者ＩＤ候補生成処理は、すべての利用者ＩＤに対して行われ、ｘ≧ｙとなるｊが全て結託者ＩＤ候補として求められる。

【０１７８】次に、図１９に示すフローチャートを用いて、上記のようにして生成された結託者ＩＤ候補について弱ＩＤか非弱ＩＤかを判定する図１８のステップＳ４７の判定処理の具体的な手順について説明する。この判定処理は、基本的に図１２に示した埋め込み符号生成部１１において利用者ＩＤ割り当て部２６における図１３の利用者ＩＤ候補判定部２６２の図１５で示した判定処理と同様であり、判定の対象が利用者ＩＤ候補から結託者ＩＤ候補に置き換わっただけである。

【０１７９】すなわち、まず図１８のステップＳ４６で決定された結託者ＩＤ候補を一つずつシーケンシャルに

入力し（ステップＳ６１）、これらの結託者ＩＤ候補が結託者ＩＤとして誤検出される確率（誤検出確率）を推定する（ステップＳ６２）。この誤検出確率の推定は、例えば先の式（９）（１０）を定義し、ある利用者ＩＤ（ｕ）が結託者ＩＤとして誤検出される確率を概ね表す量として、式（１１）または式（１２）の評価値ＥＥＦを計算することによって行う。次に、ステップＳ６２で推定された誤検出確率（例えば、式（１１）または（１２）のＥＥＦ）が所定の閾値を超えたか否かを調べ（ステップＳ６３）、閾値を超える場合は、結託者ＩＤ候補が弱ＩＤであると判定し（ステップＳ６４）、また誤検出確率が閾値以下の場合は、結託者ＩＤ候補が非弱ＩＤであると判定する（ステップＳ６５）。

【０１８０】図２０は、本実施形態において各パラメータがＬ＝７．３４×10^6、ｃ＝３２、ＥＥＦ＝０．０００００１、ｋ＝２、p_0＝５１２、ｚ＝１１、ｋ′＝２０８、ｎ＝２．６３×10^5の場合に、実際の結託者ＩＤに対して検出される結託者ＩＤと、先の合同式充足数（ｘ）と、検出結果の正誤（１が正検出、０が誤検出）を示している。

【０１８１】この例では、ｋ＋ｚ＝１３であるので、第１の実施形態では実際の結託者ＩＤのうちＩＤ＝４７８２４だけが結託者ＩＤとして検出される。これに対し、本実施形態では実際の結託者ＩＤのうち、それが非弱ＩＤであって、かつ充足式数ｘが比較的多いＩＤは正しく結託者ＩＤとして検出される。図２０の例では、結託者ＩＤのうち例えば３桁を超えるＩＤを非弱ＩＤとすれば、これらの非弱ＩＤのうち充足式数ｘが１０以上のものは、全て結託者ＩＤとして検出される。

【０１８２】図２１は、本実施形態においてパラメータＬ、ｃ、ＥＥＦ、ｋ、p_0、ｚ、ｋ′及びｎのうち結託者数ｃ以外は図２０と同じにし、ｃ＝６４とした場合に、実際の結託者ＩＤに対して検出される結託者ＩＤと、先の合同式充足数（ｘ）と、検出結果の正誤（１が正検出、０が誤検出）を示している。結託者数ｃが図２０の場合の２倍となっているので、第１の実施形態では結託者ＩＤを検出することはできない。これに対し、図２１の例では、結託者ＩＤのうち例えば５桁以上のＩＤを非弱ＩＤとすれば、これらの非弱ＩＤのうち充足式数ｘが６以上のものは、全て結託者ＩＤとして検出される。

【０１８３】このように本実施形態によると、以下の効果を得ることができる。

（１）より大きな結託者数ｃに対しても、結託者数を特定できる。言い換えれば、想定する最大の結託者数が同じならば、第１の実施形態に比較してより短い符号長の埋め込み符号を実現することができる。

（２）複数の結託者ＩＤを特定できる。

（３）埋め込み符号に結託攻撃以外のノイズ（例えば、ランダムノイズ）が加わっても、結託者を特定できる。

【０１８４】ここで、（１）（２）は前述した通りである

が、(3)の効果について補足すると次の通りである。埋め込み符号(透かし情報)に例えばコンテンツ全体にわたってランダムなノイズが加わると、成分符号の復号時に誤った剰余を出力する符号が生じることがある。このようなランダムノイズによる誤り率がある程度までならば、正しい剰余対の数の方が圧倒的に多い。従って、上述した合同式充足数は、誤った結託者ＩＤ候補よりも正しい結託者ＩＤ候補の方が大きいため、結託者ＩＤの誤検出率は小さいことになる。

【０１８５】(第３の実施形態)図２２に、本発明の第３の実施形態における埋め込み符号生成部１１の構成を示す。本実施形態の埋め込み符号生成部１１では、図３に示した構成にデータベース参照部２８及び非弱ＩＤデータベース２９が追加されている。

【０１８６】非弱ＩＤデータベース２９は、全ての利用者ＩＤ候補のうち非弱ＩＤを格納している。この非弱データベース２９に格納される非弱ＩＤは、第２の実施形態の利用者ＩＤ候補判定部２６２における判定方法と同様の方法、例えば図１５で説明したアルゴリズムによって全ての利用者ＩＤ候補について弱ＩＤか非弱ＩＤかの判定を行うことによって得られる。

【０１８７】データベース参照部２８は、利用者特定情報が入力されると、この利用者特定情報に対応して非弱ＩＤデータベース２９内の一つの非弱ＩＤを利用者ＩＤとして割り当て、その非弱ＩＤ（利用者ＩＤ）を出力する。この利用者ＩＤに対して、第１及び第２の実施形態と同様に剰余計算部２２－１～２２－ｋ′、成分符号生成部２４－１～２４－ｋ′及び符号連接部２５により順次処理が行われることによって、埋め込み符号が生成される。

【０１８８】非弱ＩＤデータベース２９には、データベース参照部２８で利用者特定情報にどの非弱ＩＤを割り当てたかを示す情報が併せて格納される。すなわち、非弱ＩＤデータベース２９に格納される非弱ＩＤのうち、既に利用者特定情報に対して利用者ＩＤとして割り当てられた非弱ＩＤには、対応する利用者特定情報が対応付けて格納される。これにより以後に入力される利用者特定情報には、既に他の利用者特定情報に対して割り当てが行われた非弱ＩＤは割り当てられない。

【０１８９】このように本実施形態の埋め込み符号生成部１１によると、非弱ＩＤ、すなわち全ての利用者ＩＤのうちで結託者ＩＤとして誤検出される可能性の低い利用者ＩＤを予め求めて、これらを非弱ＩＤデータベース２９に格納しておき、この非弱ＩＤデータベース２９を参照して利用者特定情報に対する利用者ＩＤの割り当てを行うため、第２の実施形態と同様の利用者ＩＤ割り当て処理を少ない処理量で、短時間に実現することができる。

【０１９０】図２３は、本実施形態における埋め込み符号検出部１４の構成を示している。本実施形態の埋め込み符号検出部１４は、図１６に示した利用者特定情報／利用者ＩＤ対応テーブル２７と結託者特定情報生成部４８に代えて、非弱ＩＤデータベース２９とデータベース参照部４９が追加されている。

【０１９１】非弱ＩＤデータベース２９は、図２２で説明した通りであり、非弱ＩＤと利用者特定情報を対応付けて格納している。データベース参照部４９は、結託者ＩＤ候補生成部４７から結託者ＩＤ候補が入力されると、非弱ＩＤデータベース２９に格納されている非弱ＩＤのうち、結託者ＩＤ候補のいずれかに合致する非弱ＩＤを結託者ＩＤと決定し、その非弱ＩＤに対応する利用者特定情報を非弱ＩＤデータベース２９から読み出して、これを結託者特定情報として出力する。

【０１９２】本実施形態の埋め込み符号検出部１４によると、非弱ＩＤ、すなわち全ての利用者ＩＤのうちで結託者ＩＤとして誤検出される可能性の低い利用者ＩＤを予め求めて、これらを非弱ＩＤデータベース２９に格納しておき、この非弱ＩＤデータベース２９を参照して結託者ＩＤの計算と結託者ＩＤに対応する利用者特定情報の算出を行うため、第２の実施形態と同様の結託者ＩＤ計算の処理を少ない処理量で、短時間に実現することができる。

【０１９３】ここでは、非弱ＩＤを弱ＩＤと判別するために非弱ＩＤデータベース２９を用いたが、回路やプログラムとして弱ＩＤと非弱ＩＤとの判別を行うようにしてもよい。特に、結託者ＩＤが分かればそれから結託者を特定することが本発明以外の手段により可能である場合には、単に弱ＩＤの排除のみを行えばよい。

【０１９４】(第４の実施形態)次に、本発明の第４の実施形態として、ある条件の下で実現できる、第２の実施形態よりも短い符号サイズのc-secure符号による電子透かし埋め込み装置及び検出装置について説明する。

【０１９５】図２４は、本実施形態に係る電子透かし埋め込み装置における埋め込み符号生成部の構成を示すブロック図である。この埋め込み符号生成部は、利用者ＩＤを入力して同値類に基づく成分符号を生成する成分符号生成部６１－１，６１－２，…，６１－ｋ′と、これらの各成分符号を一つの符号に連接することによって、透かし情報である埋め込み符号を生成する符号連接部６２からなる。

【０１９６】図２５に、図２４に示した同値類に基づく成分符号生成部６１－１，６１－２，…，６１－ｋ′の一つ(６１－ｉ)の構成を示す。以下、Ｚ／ｐＺ＝｛０，１，２，…，ｐ－１｝とする。成分符号生成部６１－ｉは、$(Z/pZ)^k$内対応点計算部６１１と同値類要素番号計算部６１２及び成分符号生成部６１３によって構成される。

【０１９７】Z_p^k内対応点計算部６１１は、利用者ＩＤを入力して、対応するZ_p^k内の点を出力する。利用者ＩＤＩＤ(u)と$(Z/pZ)^k$内の点$(u_0, u_1, u_2,$

…，u_{p-1}）との対応付けは、例えば、$u=u_0+u_1p+\cdots+u_{k-1}p^{k-1}$によって行う。ある集合Ｕの要素に間に同値関係Ｒがあるとき、その同値関係Ｒによってある要素ｕと同値なもの全体の集合をその要素ｕの同値類と呼ぶ。Ｕの同値関係Ｒに関する同値類全体からなる集合をＵ／Ｒで表し、ＵのＲに関する同値類という。（Ｚ／ｐＺ）ｋの要素の間にある平行移動Ｔによって、同値関係R_Tが定義できる。そして、この同値関係R_Tに関する同値類が定義できる。

【０１９８】一つの同値類に属する要素に対して、０から$p^{k-1}-1$まで番号（これを同値類要素番号と呼ぶことにする）を割り振ることができる。同値類要素番号計算部６１２は、この同値類番号を計算して部分ＩＤとして出力する。すなわち、本実施形態では入力された利用者ＩＤに対する整数要素の組として、同値類要素番号計算部６１２により同値類要素番号が計算される。成分符号生成部６１３は、同値類要素番号計算部６１２で計算された部分ＩＤから成分符号を生成する。

【０１９９】図２６は、平行移動による同値類の例を示す図である。これはｐ＝７，ｋ＝２の例である。平行移動（１，６）と平行移動（３，４）は、斜線部で示される格子によって構成されている同じ同値類を定義していることが分かる。

【０２００】図２７は、図２６のｐ×ｐの格子を周期的に繰り返したとき、同値類がどのように表されるかを示す図である。平行移動による同値関係によって定義される同値類であって、（０，０）の格子を含む同値類は、ある傾きを持った直線上に乗っていることが分かる。図２８は、図２６をｋ＝３に拡張した場合の例を示す図である。

る。同様にして、任意の正整数ｋに対して平行移動による同値関係によって同値類を定義することができる。

【０２０１】一つの同値類に含まれる元の個数は、ｐ個である。順序番号（同値類内要素番号）は、このｐ個の元に対して与えられる。一方、商集合の要素の個数（＝同値類の個数）は$p^k/p=p^k-1$である。従って、順序番号を指定すると、p^k-1個の元が指定されることになる。この順序番号が部分ＩＤとして成分符号によって符号化されることになる。

【０２０２】ここで、同値類要素番号計算部６１２での同値類要素番号（部分ＩＤ）の割当て方法について述べる。この割当て方法として、次の２通りが考えられる。

【０２０３】（割当て方法１）　同値関係R_Aに関する同値類に対して割り当てた番号である同値類番号を用いる方法であり、０から$p^{k-1}-1$までの番号が割り当てられる。

【０２０４】（割当て方法２）　同値類の要素に対して割り当てた番号を用いる方法であり、０からｐ－１までの番号が割り当てられる。

【０２０５】これらのうち割当て方法２がより好ましい。この割当て方法１を採用した場合には、第２の実施形態と同様の議論が展開できるため、先の式（６）が成立する。つまり、式（６）と後述する式（２２）の両者を満足するような符号を採用すれば良い。この割当て方法２の例を挙げる。平行移動$A_i=(a_{i,0}, a_{i,1}, \cdots, a_{i,k-1})$による同値類の場合、$u=(u_0, \cdots, u_{k-1})$は、同値類要素番号（部分ＩＤ）として次式が割り当てられる。

【０２０６】

【数２２】

$$\sum_{j=0}^{k-1} u_j a_{i,j} \bmod p \qquad (15)$$

【０２０７】図２９に、本実施形態に係る電子透かし検出装置における埋め込み符号検出部の構成を示す。この埋め込み符号検出部は、符号分割部７１、同値類に基づく成分符号復号部７２－１，７２－２，…，７２－ｋ′及び結託者ＩＤ計算部７３から構成されている。

【０２０８】図示しない埋め込み符号抽出部により、入力された検出対象コンテンツ（埋め込み済みコンテンツ）から透かし情報（埋め込み符号）が抽出され、この抽出された透かし情報である埋め込み符号が符号分割部７１により各成分符号に分割された後、同値類に基づく成分符号復号部７２－１，７２－２，…，７２－ｋ′により復号されることにより、利用者ＩＤに対応する同値類要素番号の対が生成される。こうして生成された各同値類要素番号の対から、結託者ＩＤ計算部７３で結託者ＩＤが計算され、結託者が特定される。

【０２０９】なお、第１、第２の実施形態と同様に、同値類要素番号の対の一方から利用者ＩＤ計算部により利用者ＩＤを求め、また各同値類要素番号の対から結託判定部により結託の有無を判定し、その結託判定部判定結果について、結託判定ＯＲ部で論理和をとることにより、結託が存在したか否かを最終的に判定して、結託が存在すると判定されたときに結託者ＩＤ計算部７３で結託者ＩＤを計算する構成としてもよい。

【０２１０】図３０は、同値類に基づく成分符号復号部７２－１，７２－２，…，７２－ｋ′の一つ（７２－ｉ）の構成を示している。同値類に基づく部分復号部７２－ｉは、後述するランダム誤りを許容する検出アルゴリズム３に基づくものであり、ブロック分割部７２０、“１”ビット計数部７２１、“＞t_0”判定部７２２、“＜$d-t_0$”判定部７２３、最小位置決定部７２４及び最大位置決定部７２５から構成される。

【０２１１】ブロック分割部７２０は、入力された成分符号を各ブロックへ制限したものに分割して分割結果をそれぞれ“１”ビット計数部７２１へ出力する。“１”ビット計数部７２１は、“１”が立っているビットの数を計数して、その計数値を“＞t_0”判定部７２２及び

“＜ｄ－ｔ0”判定部７２３へそれぞれ出力する。

【０２１２】“＞ｔ0”判定部７２２は、入力が第１の閾値ｔ0より大きいか否かを判定し、真ならば１、偽ならば０をそれぞれ出力する。“＜ｄ－ｔ0”判定部７２３は、入力が第２の閾値ｄ－ｔ0より小さいか否かを判定し、真ならば１、偽ならば０をそれぞれ出力する。

【０２１３】最小位置決定部７２４は、“＞ｔ0”判定部７２２からの入力ビットの組のうち１が立っている最小のビット番号を出力する。最大位置決定部７２５は、“＜ｄ－ｔ0”判定部７２３からの入力ビットの組のうち１が立っている最大のビット番号を出力する。

【０２１４】ここで、図２９の電子透かし検出装置において埋め込み符号である透かし情報の復号時に誤りが生ずる可能性がある場合について説明する。埋め込み符号の復号時に誤りがある場合には、誤った利用者を結託者と特定するおそれがある。この誤りを防ぐには２通りの方法がある。

【０２１５】(方法１)　電子透かし埋め込み装置において、埋め込み符号に対して誤り訂正符号化を行ってから埋め込みを行い、電子透かし検出装置において検出された符号に対して誤り訂正復号を行う。

(方法２)　図２９の成分符号復号部７２－１，７２－２，…，７２－ｋ′に誤りを許容する性質を持たせる。

【０２１６】本実施形態では、(方法２)を採用する。抽*

*出された埋め込み符号には誤り確率のランダムな誤りが加わっていると仮定する。第２の実施形態で述べた検出アルゴリズム１に改良を加えた以下のような検出アルゴリズム３を用いることで、誤りを許容する。

【０２１７】(検出アルゴリズム３)

(1)検出された符号ｘ∈｛0，1｝lを入力する。ここで、ｚ＝(ｎ－1)ｄとする。

(2)ｓ＝0からｎ－２まで、以下を実行する：

(2－1)もし、weight(ｘ|Bs)＞0ならば、中断する。

(3)ｔ＝ｎ－２からｓまで、以下を実行する：

(3－1)もし、weight(ｘ|Bt)＜ｄ－ｔ0ならば、中断する。

(4)ｓとｔを出力する。

ここでｔ0は、この検出アルゴリズム３の誤りに対する許容性を表すパラメータである。

【０２１８】次に、結託による埋め込み符号の改竄があったことを判定する閾値として、新たなパラメータを加える意味について説明する。埋め込み符号のうち、結託によっては改竄んが行われなかったブロックに対して、結託以外の原因でランダムな誤りが発生した場合、ｔ0＋１ビット以上の反転が生ずる確率は、次式で与えられる。

【０２１９】

【数２３】

$$\varepsilon_1 = \sum_{i=t_0+1}^{d} {}_dC_i (1-\varepsilon_0)^{d-i} \varepsilon_0^{\,i} < e^{-\frac{(t_0-d\varepsilon_0)^2}{d}} \qquad (16)$$

※は、次式より小さい。

【０２２０】一方、結託によって改竄が行われたブロックに対して、結託以外の原因でランダムな誤りが加法的に加わった場合、ｔ0ビット以下の反転が生ずる確率

【０２２１】

【数２４】

$$\varepsilon_2 = \sum_{i=0}^{t_0} {}_dC_i (1/2)^d < e^{-\frac{\left(\frac{d}{2}-t_0\right)^2}{d}} \qquad (17)$$

【０２２２】ランダム誤りのために埋め込み符号を誤って検出をしてしまう確率は、少なくとも一つのブロックにおいて誤った検出をする確率以下であり、この確率は、

$\varepsilon_3 = 1-(1-\varepsilon_1)^{n-1}(1-\varepsilon_2)^2 < (n-1)\varepsilon_1 + 2\varepsilon_2$

で表される。図３１に示すようにｔ0を適当に選択することで、加法的にランダムな誤りが加わった場合にも、検出誤りを小さく設定できる。図３０に示した成分符号復号部７２－ｉは、上述したようなランダム誤りを許容する先の検出アルゴリズム３に基づく処理を行う。

【０２２３】図３２に、結託者ＩＤ計算部７４の構成を示す。結託者ＩＤ計算部７４は、同値類選択部８１、一貫性検査部８２及び候補ＩＤ計算部８３から構成される。

【０２２４】同値類要素選択部８１は、ｋ′個の同値類要素番号の対の各々から一方の同値類番号を選択して一貫性検査部８２へ出力し、一貫性検査部８２から次候補の要求を受けると、同値類要素番号の新たな組を選択する。

【０２２５】一貫性検査部８２は、ｋ′個の組から(ｋ＋１)個の組を選択し、その同値類要素番号の組が真に一貫しているか否かを検査する。この検査は、(ｋ＋１)個のうちｋ個の同値類要素番号を候補ＩＤ計算部８３に渡し、返された候補ＩＤが残りの同値類要素番号の示す同値類番号と矛盾していないか否かを判定することにより行われる。残りの個のすべての同値類番号に対して、この判定が矛盾していないという結果ならば、この候補ＩＤを結託者ＩＤとして出力し、そうでない場合には、次候補を一貫性検査部８２に要求する。

45

【０２２６】ここで、図３２中の候補ＩＤ計算部８３においてｋ個の同値類要素番号から結託者ＩＤを再構成する方法を示す。例えば、ｋ個の平行移動$A_{i(0)}$，…，$A_{i(k-1)}$に対して、同値類要素番号がr_0，…，r_{k-1}で与

*えられた場合、次式の連立合同方程式が成り立つ。

【０２２７】

【数２５】

$$\sum_{j=0}^{k-1} u_j a_{i(v),j} \equiv r_v \bmod p \qquad (18)$$

【０２２８】ｋ次正方行列$(a_{i(v),j})$が正則ならば、逆行列$(a^{-1}{}_{j,i(v)})$が存在する。この場合、次式によって利用者ＩＤが得られる。

※【０２２９】

【数２６】

$$u_j \equiv \sum_{v=0}^{k-1} a^{-1}{}_{ji(v)} r_v \bmod p \qquad (19)$$

【０２３０】一般には、正則性が満たされるとは限らない。正則性が満足されない場合には、利用者ＩＤは一意に決まらず、結託者ＩＤを含む利用者ＩＤの集合が得られる。この集合は、ｐのべき乗の大きさを持つ。正則性を満たさない成分符号の組はあらかじめ分かっているので、結託者ＩＤの候補の計算には、選択しないような構成もできる。

★【０２３１】図３２中の一貫性検査部８２は、こうして得られた結託者ＩＤの候補(を含む集合に対して)と、さらにｚ個の同値類要素番号r_k，…，r_{k+z-1}との間の一貫性を検証する。それは、ｖ＝０，…，ｚ－１に対して、次式が成立することを確認することで行われる。

【０２３２】

【数２７】

$$\sum_{j=0}^{k-1} u_j a_{i(k+v),j} \equiv r_{k+v} \bmod p \qquad (20)$$

【０２３３】本実施形態によると、第１、第２の実施形態と同様に結託攻撃への耐性を有し、かつ３人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することが可能となる。以下、詳細に説明する。

【０２３４】まず、ｐを正整数とする。すなわち、本実施形態では第２の実施形態におけるp_i（ｉ＝１，２，…，ｋ′）(所定個数ｎの利用者ＩＤに対して計算される剰余の値の個数)に相当する個数(所定個数ｎの利用者ＩＤに対して計算される整数要素の値の個数)を同一の正整数ｐとしている。そして、利用者ＩＤｕを$u=u_0+u_1p+\cdots u_{k-1}p^{k-1}$に従って、$(u_0, u_1, \cdots, u_{k-1}) \in (Z/pZ)^k$で表現する。また、$k'=c(k+z)/2$とし、$p^k \geqq n$とする。

【０２３５】空間$Z_p{}^k$の平行移動$A \equiv (a_0, a_1, \cdots, a_{k-1})$に関する同値関係$R_A$を以下のように定義する。

$R_A((u_0, u_1, \cdots, u_{k-1}), ((u_0', u_1', \cdots, u_{k-1}'))$

$\longleftrightarrow$ $u_0' \equiv u_0+a_0 \bmod p$,

$u_1' \equiv u_1+a_1 \bmod p \cdots$,

$u_{k-1}' \equiv u_{k-1}+a_{k-1} \bmod p$

$jA-(ja_0 \bmod p, ja_1 \bmod p, \cdots, ja_{k-1} \bmod p)$とすると、ｊがgcd(ｊ，ｐ)＝１を満たすときには、R_AとR_{jA}とは同じ同値関係を与える。

【０２３６】利用者全体の集合を$U=(Z/pZ)^k$の同値関係R_Aに関する商集合U/R_Aが定義できる。この商集合の個々の元は同値類と呼ばれ、同値関係R_Aによって同一視された元の集合である。すべての同値類に対して、それに含まれる元に順序番号を与えることにより、ある番号を指定することで、各同値類から１個ずつ元を選択できる。

【０２３７】ｋ′（ｋ′≧ｋ）個の平行移動$A_0, \cdots, A_{k'-1}$を用意すると、それぞれに対して商集合$Q_i=U/R_{Ai}$（ｉ＝０，…，ｋ′－１）が定義される。各商集合に対して、上に述べた順序番号を定義する。

【０２３８】次に、ｋ′個の商集合中の任意のｋ個の商集合のそれぞれに対して、順序番号を指定することで、利用者を一意に特定できるような商集合の組を構成するために、以下のような条件を仮定する。

【０２３９】(条件１)　商集合の大きさを等しいとする。すべての$A_i=(a_{i,0}, \cdots, a_{i,k-1})$（ｉ＝０，…，ｋ′－１）において、すべての$a_{i,m}$(m＝０，…，ｋ－１)に対して、$\gcd(a_{i,m}, p)=1$または$a_{i,m}=0$であるとする。これにより、$jA_i=(0 \bmod p, \cdots, 0 \bmod p)$を満たす最小の正整数ｊはｐとなる。

(条件２)　２つの平行移動A_i, A_i'に対して、$jA_i=j'A_i'$が成立する正整数$j<p, j'<p$が存在しない。ｐが素数の場合、このような条件を満たす平行移動の個数は、次のように数え上げることができる。まず、(条件１)より各平行移動の成分の値がｐと互いに素の関係にある場合の数は、$\phi(p)=p-1$で表される。ここで、φはオイラー関数である。これに０である場合を加えて、各成分がとりうる値の場合の数は、ｐである。従って、平行移動として許される場合の数は、(p^k-1)

47

個である。ここで、－１は、(0, 0, …, 0)を除外したことによる。ところが、これらの中には(ｐ－１)個ずつ互いに他の整数倍(１倍、２倍、…、(ｐ－１)倍)となっているものがある。従って、実際に、相異なる商集合を定義する平行移動として独立なものは、(ｐ^k－１)／(ｐ－１)個となる。

【０２４０】また、(条件２)に関しては、仮にある２つの平行移動Ａ$_i$, Ａ$_i$′が(条件２)の制約を満たさないと＊

48

＊する。つまり、正整数ｊ＜ｐ, ｊ′＜ｐに対してｊＡ$_i$＝ｊ′Ａ$_i$′とすると、ｐが素数の場合には、これは互いに他の整数倍で表現できることを意味する。よって、(条件１)に対して数え上げた独立な平行移動は、そのまま(条件２)を満足する。平行移動の組は、次のように具体的に構成できる。

【０２４１】

【数２８】

$$\begin{aligned}
A_1 &= (0,0,\cdots,0,1),\\
A_2 &= (0,0,\cdots,0,1,0),\\
&\vdots\\
A_{1+p} &= (0,0,\cdots,0,1,p-1),\\
A_{1+p+1} &= (0,0,\cdots,0,1,0,0),\\
&\vdots\\
A_{1+p+p^2} &= (0,0,\cdots,0,1,p-1,p-1),\\
&\vdots\\
A_{1+p+p^2+\cdots+p^{k-2}+1} &= (1,0,\cdots,0),\\
&\vdots\\
A_{1+p+p^2+\cdots+p^{k-1}} &= (1,p-1,\cdots,p-1).
\end{aligned} \qquad (21)$$

【０２４２】ｐが素数でない場合についても、(条件１)(条件２)を満足するように平行移動を選択すれば、同様の構成が可能である。

【０２４３】上述したような平行移動の組によって商集合を構成し、各商集合の同値類の元に順序番号を定義することで、中国剰余定理に基づく符号の場合と同様の符※号を構成できる。この符号が誤りεを持つc-secure符号となるためには、定理２が成立することに加えて、以下の条件が満たされなければならない。

【０２４４】

【数２９】

$$k' = \frac{c}{2}(k+z) \le \frac{p^k-1}{p-1} \qquad (22)$$

【０２４５】この場合、全ての因数は同じ大きさのｐであるので、ｐ$_{ave}$＝ｐである。

【０２４６】このように本実施形態によると、成分符号として式(２１)で示されるような平行移動によって定義される同値類に基づく符号を生成して、この成分符号を連接することで、第１、第２の実施形態よりも短い符号サイズのc-secure符号による埋め込み符号を生成し、その埋め込み符号を検出する場合において、第２の実施形態で規定した条件式ｋ′≧ｃ(ｋ＋ｚ)／ｑや式(８)の条件に加え、さらに式(２２)の条件を満足するようにすることによって、結託攻撃への耐性を有し、かつ３人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成し、かつその埋め込み符号を正しく復号することができる。

【０２４７】(第５の実施形態)次に、本発明の第５の実施形態として、埋め込み済みコンテンツの品質への影響を小さく抑えるように、従来よりも最適な符号化が行われる電子透かし埋め込み装置及び検出装置について説明する。

【０２４８】図３３に、本実施形態に係る電子透かし埋め込み装置の構成を示す。この電子透かし埋め込み装置は、シンプレックス符号生成部９１、符号語選択部９２及び電子透かし埋め込み部９３から構成されている。

【０２４９】シンプレックス符号とは、符号長ｎ－１、符号語数ｎで、符号語間の相互相関が－１／(ｎ－１)となる符号であり、ｎ次のアダマール(Hadamard)行列を基に構成することができる。すなわち、符号語がｎ－１次元ユークリッド空間中のｎ－１次元単体の頂点に位置するような符号がシンプレックス符号である。例えば、３次元ユークリッド空間の場合は、図３４に示すように(-1, -1, 1), (1, -1, -1), (-1, 1, -1)で示す３つの頂点に位置する符号がシンプレックス符号を構成する。

【０２５０】シンプレックス符号生成部９１では、このようなシンプレックス符号の符号語を生成する。シンプレックス符号生成部９１は、あらかじめ生成された符号語の表を記憶したものであってもよい。符号語選択部９２は、生成されたシンプレックス符号に順番を割り振っておき、与えられた利用者ＩＤに対応する符号語を選択して出力する。なお、シンプレックス符号生成部９１及び符号語選択部９２の部分は、利用者ＩＤが入力されてから、利用者ＩＤに対応するシンプレックス符号の符号語を生成して出力するように構成されていてもよい。

【０２５１】電子透かし埋め込み部９３は、符号語選択部９２より受け取った符号語を透かし情報として埋め込み対象コンテンツに埋め込む。埋め込みは、スペクトラム拡散によって行う。

【０２５２】図３５に、図３３に示した電子透かし埋め

込み装置に対応する本実施形態に係る電子透かし検出装置の構成を示す。この電子透かし検出装置は、シンプレックス符号生成部１０１、符号語選択部１０２、相関値計算部１０３及び相関値判定部１０４から構成されている。シンプレックス符号生成部１０１と符号語選択部１０２については、図３３で説明した電子透かし埋め込み装置の中のそれと同一であるため、説明を省略する。

【０２５３】相関値計算部１０３では、入力された埋め込み済みコンテンツと入力された利用者ＩＤに基づいて符号選択部１０２で選択された符号語との間の相関値を計算する。相関値判定部１０４では、相関値計算部１０３により計算された相関値がある閾値を超えているか否かによって、符号選択部１０２からの符号語が埋め込み済みコンテンツに埋め込まれているか否かを判定し、検出／非検出信号を出力する。

【０２５４】このように本実施形態に係る電子透かし埋め込み／検出装置によれば、任意の対の間での相互相関値が小さくなるようなシンプレックス符号の符号語を擬似乱数系列として用い、これを透かし情報として埋め込んでいる。従って、透かし情報として別の利用者ＩＤに対応する符号語が埋め込まれていると誤判定を行う確率は非常に小さくなる。

【０２５５】(第６の実施形態)次に、本発明の第６の実施形態として、第５の実施形態の電子透かし検出装置を応用して結託攻撃に対する結託者特定機能を持たせた電子透かし検出装置ついて説明する。図３６は、本実施形態に係る結託者特定機能に係る部分の構成を示している。

【０２５６】この電子透かし検出装置は、結託者特定機能を持たせるために、シンプレックス符号生成部１１１、符号語選択部１１２、相関値計算部１１３、利用者ＩＤ生成部１１４、相関値ベクトルノルム計算部１１５、電子透かし判定部１１６及び結託者判定部１１７を有する。シンプレックス符号生成部１１１、符号語選択部１１２及び相関値計算部１１３は、図３５に示した電子透かし検出装置の中のそれと基本的に同じである。

【０２５７】利用者ＩＤ生成部１１４では、予め登録されたすべての利用者ＩＤを生成する。符号語選択部１１２では、これらすべての利用者ＩＤに対応するシンプレックス符号の符号語が選択され、これらの各符号語と図示しない埋め込み済みコンテンツとの相関値が相関値計算部１１３で計算される。

【０２５８】相関値ベクトルノルム計算部１１５では、すべての利用者ＩＤに対して計算された相関値をベクトルとみなして、そのノルムを計算する。この相関値ベクトルノルムは、例えばすべての相関値の和とする。

【０２５９】電子透かし判定部１１６では、計算されたベクトルノルムに基づいて、例えば、このノルムがある閾値を超えるか否かにより、透かし情報が埋め込まれていたか否かを判定する。この判定の結果、透かし情報が

埋め込まれていたと判断した場合には、結託者判定部１１７において相関値ベクトルの中で最も大きな値を示した利用者ＩＤを保有する利用者を結託者として特定する。

【０２６０】また、結託者特定部１１７においては、このような方法の他、例えば相関値ベクトルがｎ－１次元単体の部分単体のうち、どの部分単体の重心を通るかを求め、その部分単体の頂点に対応する利用者ＩＤを保有する利用者を結託者とすることで、複数の結託者を特定することもできる。

【０２６１】なお、第５乃至第６の実施形態において、透かし情報として用いる擬似乱数系列として、Ｎ(0，1)のガウシアンノイズを採用する場合には、図３７に示すようにシンプレックス符号生成部１２１で生成されたシンプレックス符号を座標ランダム回転部１２２によりランダムに回転させて符号語とすればよい。

【０２６２】さらに、本発明に係る埋め込み符号生成装置は、電子透かし埋め込み装置のようにディジタルデータである埋め込み対象コンテンツの透かし情報として埋め込むための埋め込み符号のみでなく、例えば化学物質からなる合成物などに化学的に埋め込むための埋め込み符号を生成するような用途にも適用できる。その場合には、実質上その物質の構成を変化させても構わない複数の部分に対して、構成変化を施す部分を“１”、構成変化を施さない部分を“０”として、本発明に係る符号の符号語のビットを対応付けるようにする。

【０２６３】

【発明の効果】以上説明したように、本発明によればフィンガープリンティングシステムを構成する電子透かし埋め込み／検出装置において、利用者総数や結託者数が大きくなっても、小さな符号サイズの透かし情報を埋め込ことによってコンテンツの品質劣化を伴うことなく、結託攻撃に対するロバスト性を持つことができ、非可逆圧縮等の他の攻撃に対してもロバスト性を得ることができる。

【０２６４】また、本発明の電子透かし埋め込み／検出装置により、コピー制御情報や利用制御情報といった透かし情報を埋め込み、コンテンツを利用する機器を制御する場合に、同一コンテンツに対して異なる機器制御情報が埋め込まれている場合にその比較によって制御情報の改竄を行う攻撃に対してもロバスト性を有するコンテンツ利用システムを構築することも可能である。

【０２６５】さらに、本発明によると結託攻撃への耐性を有し、かつ３人以上の結託者が改竄に関与した場合においても、正しい誤り率の評価に基づいて十分かつ適切な埋め込み符号を生成する埋め込み符号生成装置及びその埋め込み符号を正しく復号する埋め込み符号検出装置を提供することができる。

【図面の簡単な説明】

【図１】　本発明に係る電子透かし埋め込み装置及び電

子透かし検出装置が適用されるフィンガープリンティングシステムの概略構成を示す図

【図２】　本発明の第１の実施形態に係る電子透かし埋め込み装置及び電子透かし検出装置の構成を示すブロック図

【図３】　図２における埋め込み符号生成部の構成を示すブロック図

【図４】　図３における成分符号生成部の構成を示すブロック図

【図５】　本発明で生成される成分符号(結託前の成分符号)の値を示す図

【図６】　図２における埋め込み符号検出部の構成を示すブロック図

【図７】　図６における結託者ＩＤ計算部の構成を示すブロック図

【図８】　図７における一貫性検査部の構成を示すブロック図

【図９】　同第１の実施形態における結託者特定アルゴリズムを示すフローチャート

【図１０】　図６における中国剰余定理部の処理の流れを示すフローチャート

【図１１】　同第１の実施形態に係る埋め込み符号検出部の処理の流れを示すフローチャート

【図１２】　本発明の第２の実施形態に係る埋め込み符号生成部の構成を示すブロック図

【図１３】　図１２における利用者ＩＤ割り当て部の構成を示すブロック図

【図１４】　図１３の利用者ＩＤ割り当て部の処理の流れを示すフローチャート

【図１５】　図１３における利用者ＩＤ候補判定部の処理の流れを示すフローチャート

【図１６】　同第２の実施形態に係る埋め込み符号検出部の構成を示すブロック図

【図１７】　図１６における結託者ＩＤ計算部の構成を示すブロック図

【図１８】　図１７における結託者ＩＤ候補生成部と結託者ＩＤ候補判定部及び結託者ＩＤ決定部の処理の流れを示すフローチャート

【図１９】　図１７における結託者ＩＤ候補判定部の処理の詳細な流れを示すフローチャート

【図２０】　同第２の実施形態において結託者総数が「３２」の場合の実際の結託者ＩＤに対して検出される結託者ＩＤと合同式充足数及び検出結果の正誤の関係を示す図

【図２１】　同第２の実施形態において結託者総数が「６４」の場合の実際の結託者ＩＤに対して検出される結託者ＩＤと合同式充足数及び検出結果の正誤の関係を示す図

【図２２】　本発明の第３の実施形態に係る埋め込み符号生成部の構成を示すブロック図

【図２３】　同第３の実施形態に係る埋め込み符号検出部の構成を示すブロック図

【図２４】　本発明の第４の実施形態に係る埋め込み符号生成部の構成を示すブロック図

【図２５】　図２４における同値類に基づく成分符号生成部の構成を示すブロック図

【図２６】　同第４の実施形態における平行移動による同値類によって商集合が定義できることを示す図

【図２７】　同第４の実施形態における平行移動による同値類の例を示す図

【図２８】　同第４の実施形態における$k=3$の場合の同値類の例を示す図

【図２９】　同第４の実施形態に係る埋め込み符号検出部の構成を示すブロック図

【図３０】　図２９における同値類に基づく成分符号復号部の構成を示すブロック図

【図３１】　図３０に示した同値類に基づく成分符号復号部について説明する図

【図３２】　図２９における結託者ＩＤ計算部の構成を示すブロック図

【図３３】　本発明の第５の実施形態に係る電子透かし埋め込み装置の構成を示すブロック図

【図３４】　本発明の第５乃至第６の実施形態で使用するシンプレックス符号について説明する図

【図３５】　同第５の実施形態に係る電子透かし検出装置の構成を示すブロック図

【図３６】　本発明の第６の実施形態に係る結託者特定機能を有する電子透かし検出装置の構成を示すブロック図

【図３７】　本発明の第５乃至第６の実施形態におけるシンプレックス符号生成部の他の例を示すブロック図

【図３８】　電子透かしに対する結託攻撃について説明する図

【図３９】　$\Gamma_0(n, d)$符号及びそれに対する結託攻撃を説明する図

【図４０】　$\Gamma_0(n, d)$符号における二つの符号間の最大距離と最小距離について説明する図

【図４１】　$\Gamma_0(n, d)$符号を用いた従来の電子透かしアルゴリズムにおける問題点を説明する図

【符号の説明】

１１…埋め込み符号生成部
１２…符号埋め込み部
１３…埋め込み符号抽出部
１４…埋め込み符号検出部
２１－１，２１－２，…，２１－ｋ′…法記憶部
２２－１，２２－２，…，２２－ｋ′…剰余計算部
２３…符号パラメータ記憶部
２４－１，２４－１，…，２４－ｋ′…成分符号生成部
２５…符号連接部
２６…利用者ＩＤ割り当て部

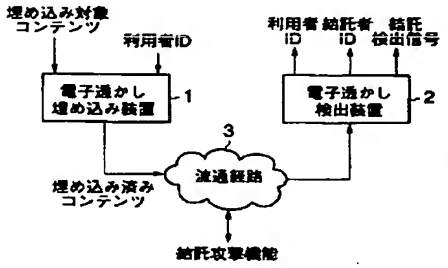
53

２７…利用者特定情報／利用者ＩＤ対応テーブル
２８…データベース参照部
２９…非弱ＩＤデータベース
４１…符号分割部
４２－１，４２－２，…，４２－ｋ′…成分符号復号部
４３…利用者ＩＤ計算部
４４－１，４４－２，…，４４－ｋ′…結託判定部
４５…結託判定ＯＲ部
４６…結託者ＩＤ計算部
４７…結託者ＩＤ計算部
４８…結託者特定情報生成部
４９…データベース参照部
５１…剰余選択部
５２…一貫性検査部
５３…中国剰余定理部
６１－１，６１－２，…，６１－ｋ′…同値類に基づく成分符号生成部
６２…符号連接部
７１…透かし情報抽出部
７２…符号分割部

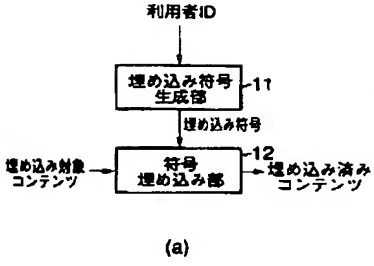
54

＊７３－１，７３－２，…，７３－ｋ′…同値類に基づく成分符号復号部
７４…結託者ＩＤ計算部
８１…同値類選択部
８２…一貫性検査部
８３…候補ＩＤ計算部
９１…シンプレックス符号生成部
９２…符号語選択部
９３…電子透かし埋め込み部
１０１…シンプレックス符号生成部
１０２…符号語選択部
１０３…相関値計算部
１０４…相関値判定部
１１１…シンプレックス符号生成部
１１２…符号語選択部
１１３…相関値計算部
１１４…利用者ＩＤ生成部
１１５…相関値ベクトルノルム計算部
１１６…電子透かし判定部
１１７…結託者特定部

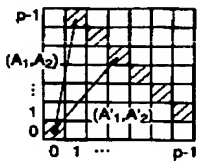
【図１】



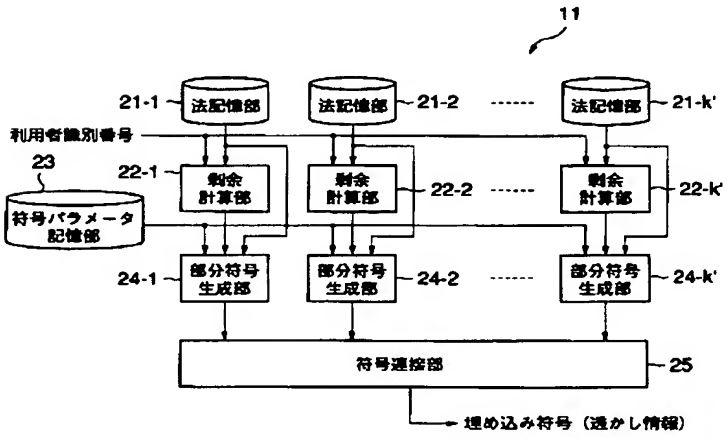
【図２】



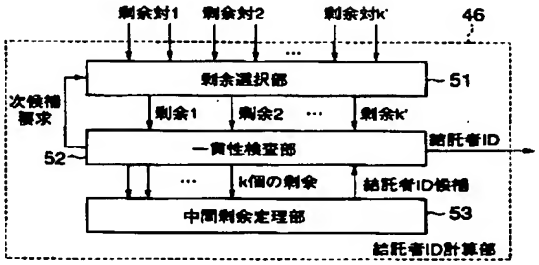
【図２６】



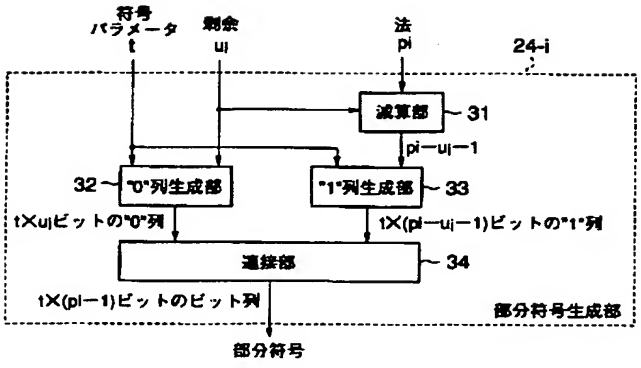
【図３】



【図７】



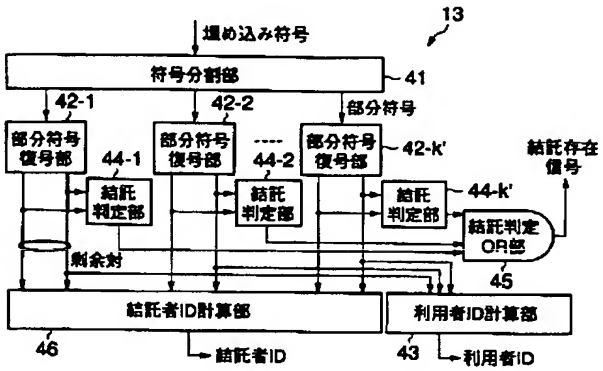
【図４】



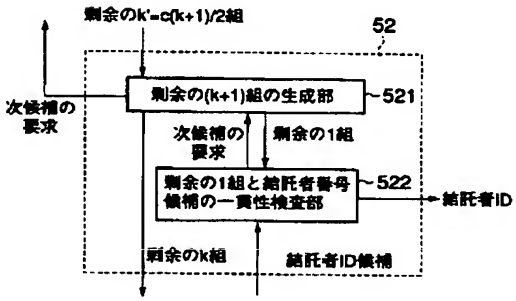
【図５】

利用者ID	B(0)	B(1)	…	B(Smin)	…	B(Smax)	…	B(n-3)	B(n-2)
0	1…1	1…1	1…1	1…1	1…1	1…1	1…1	1…1	1…1
1	0…0	1…1	1…1	1…1	1…1	1…1	1…1	1…1	1…1
…									
Smin	0…0	0…0	0…0	1…1	1…1	1…1	1…1	1…1	1…1
…									
Smax	0…0	0…0	0…0	0…0	0…0	1…1	1…1	1…1	1…1
…									
n-2	0…0	0…0	0…0	0…0	0…0	0…0	0…0	0…0	1…1
n-1	0…0	0…0	0…0	0…0	0…0	0…0	0…0	0…0	0…0

【図６】

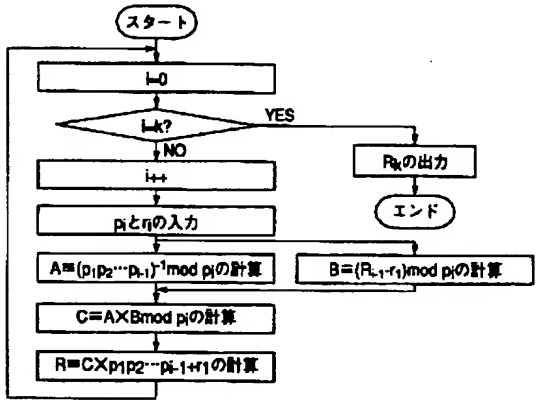


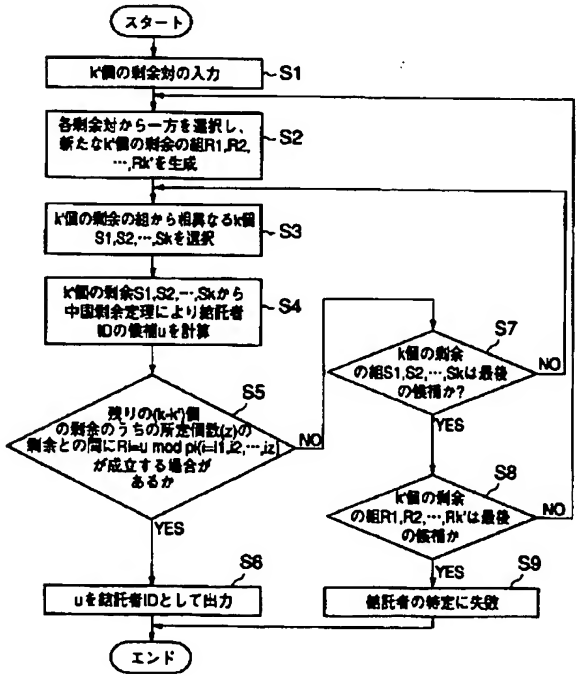
【図８】



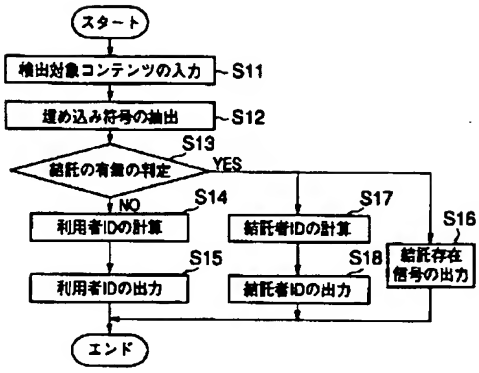
【図９】

【図１０】

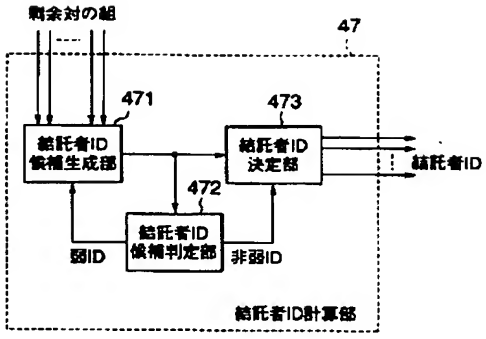




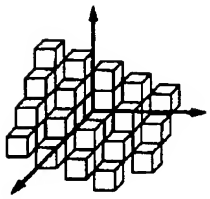
【図１１】



【図１７】

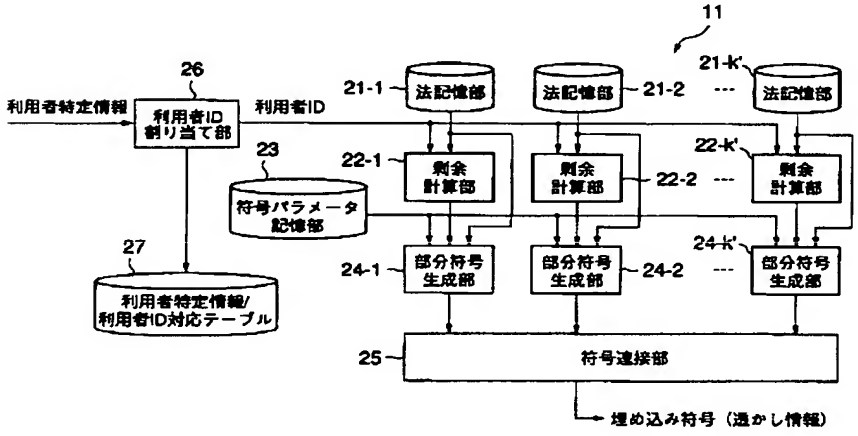


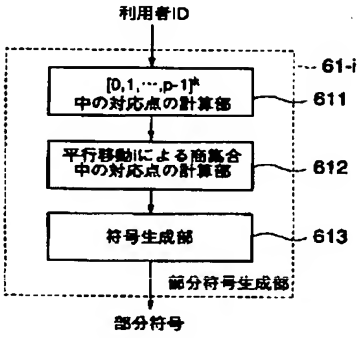
【図２８】



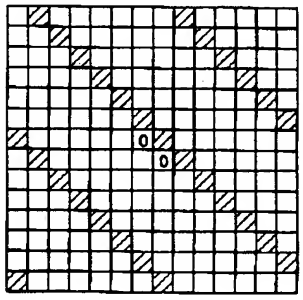
【図２５】

【図１２】

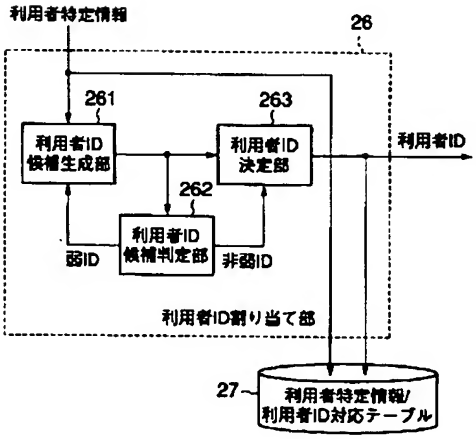




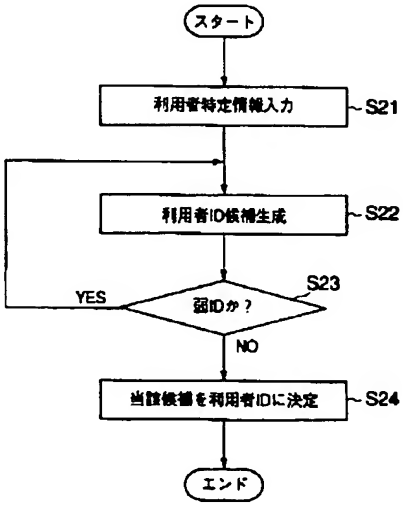
【図２７】



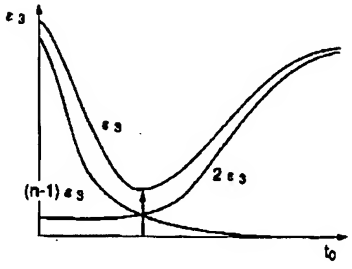
【図１３】



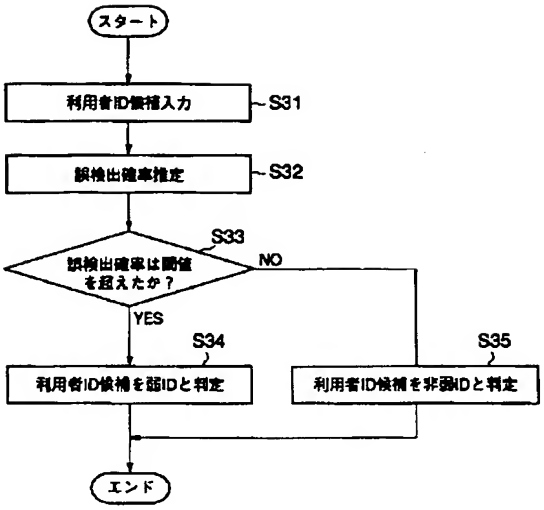
【図１４】



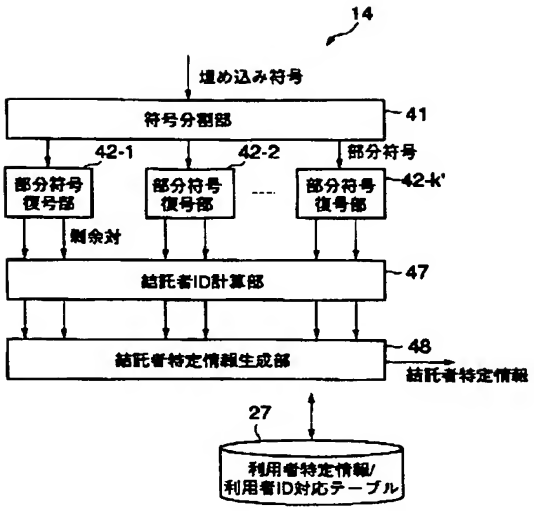
【図３１】



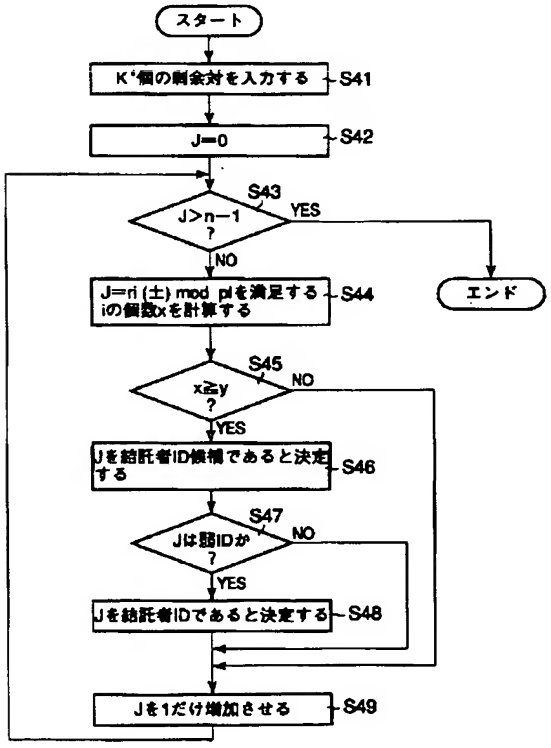
【図１５】



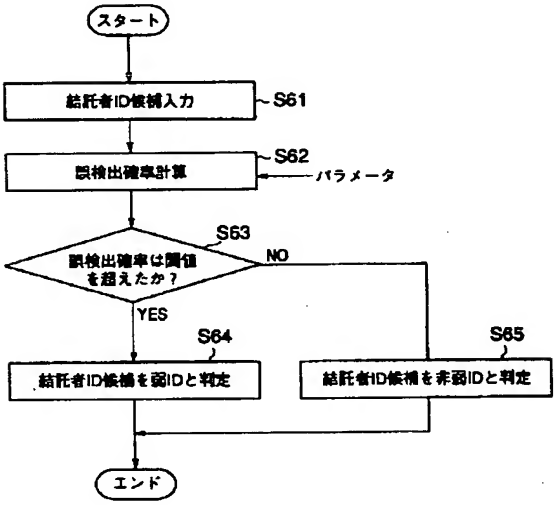
【図１６】



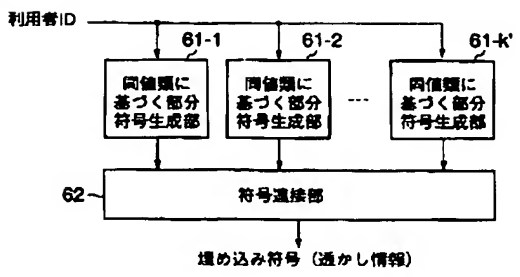
【図１８】



【図１９】



【図２４】



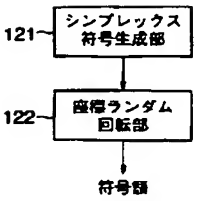
【図２０】

実際の結託者ID (c-32+0)	検出された結託者ID	合同式充足数	検出結果の正誤
3407	47824	14	1
10640	3407	12	1
15067	30374	12	1
27463	221988	12	1
30374	45380	11	1
44828	44828	10	1
45380	126166	10	1
47824	187728	10	1
52856	2	9	0
54548	52856	9	1
63547	63547	9	1
75058	175612	9	1
126166	11	8	0
133680	54546	8	1
139843	75058	8	1
143941	133680	8	1
163356	143941	8	1
164408	200009	8	1
175612	202508	8	1
187728	212493	8	1
200009	219666	8	1
202508	262123	8	1
204841	19	7	0
207450	223473	7	1
210834	3	6	0
212493	4	6	0
219666	5	6	0
221988	24	6	0
223473	38	6	0
240733	54545	6	0
253316	139843	6	1
262123	163356	6	1

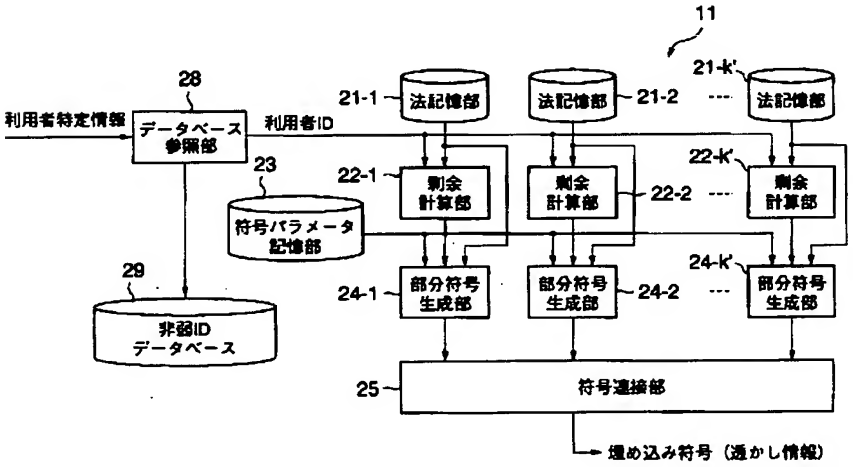
【図２１】

実際の結託者ID (c-32+32)	検出された結託者ID	合同式充足数	検出結果の正誤
2089	1	13	0
5258	4	12	0
10732	6	10	0
13913	3	9	0
26395	7	9	0
38321	10	9	0
43641	2	8	0
44196	11	8	0
48052	5	7	0
54224	9	7	0
68847	14	7	0
69827	24	7	0
70170	154324	7	1
78476	164218	7	1
83379	221793	7	1
83993	13	6	0
84045	17	6	0
94102	23	6	0
96272	96272	6	1
105743	172540	6	1
108322	16	5	0
109875	19	5	0
117337	4128	5	0
127964	6834	5	0
137307	59870	5	0
134993	66825	5	0
140009	68847	5	1
142773	76709	5	0
149815	78476	5	1
150357	81504	5	0
154324	83379	5	1
156553	97042	5	0

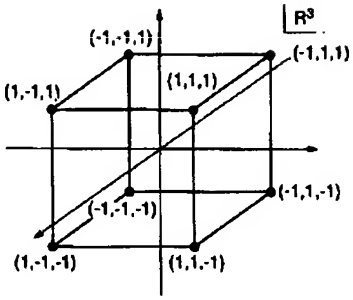
【図３７】



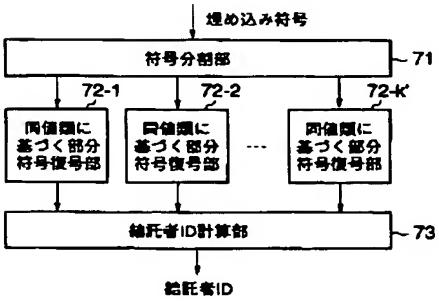
【図２２】



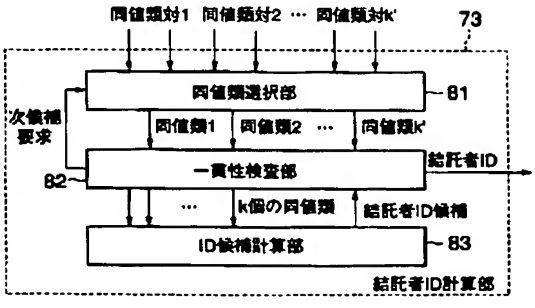
【図３４】



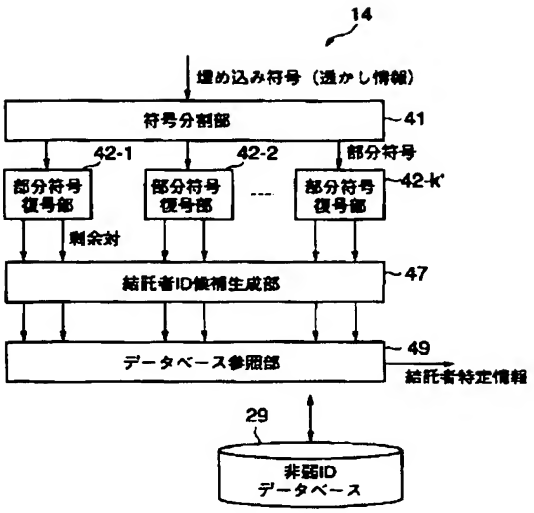
【図２９】



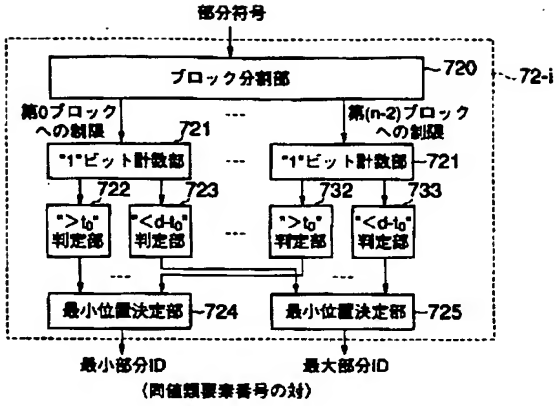
【図３２】



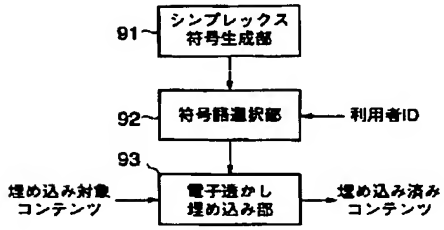
【図２３】



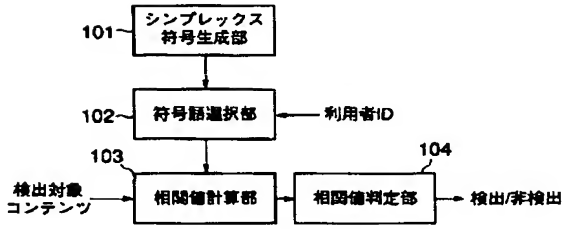
【図３０】



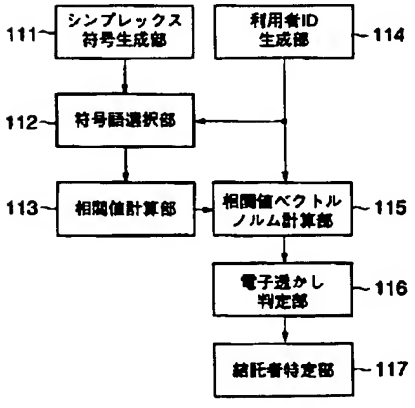
【図３３】



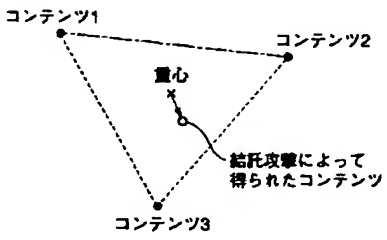
【図３５】



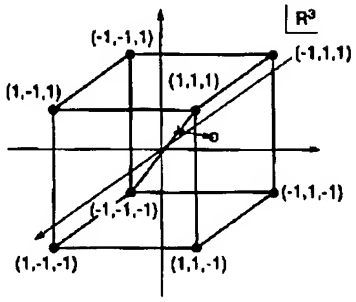
【図３６】



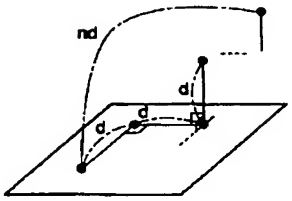
【図３８】



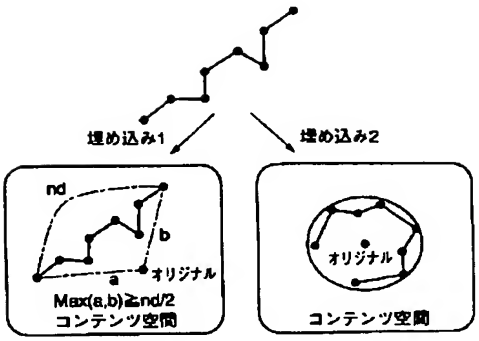
【図３９】



【図４０】



【図４１】



フロントページの続き

Ｆターム(参考) 5B057 AA20 BA01 CA01 CA08 CA12
CA16 CB01 CB08 CB12 CB16
CB19 CC02 CE08 CE09 CG07
CH08 DA06 DA17
5C063 AB03 AC01 AC05 CA23 CA36
DA07 DA13 DB09
5C076 AA14 BA06 BA09